International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Optimization in Secure Routing and Power Efficient Communication in Wireless Adhoc Network

Ugendhar Addagatla, V. Janaki

Abstract: ***Security and data propagation are the two major concerns in wireless adHoc network. The optimal routing with power conservation and traffic monitoring defines the operational efficiency of the adHoc network. Wherein energy conservation and routing security are used as a measuring parameter in controlling the traffic flow, no two parameters are defined in together to optimize the route selectivity in the network. The monitoring of routing parameter in providing secure route is governed by the characteristic optimization of forwarding link and the approach of link selection. In this paper, an approach for optimal link selection for secure routing using multi attribute monitoring and controlling of traffic flow is presented. The proposed work defines a fairness factor based on multiple monitoring attribute to control the operational efficiency of the network. The multi attribute monitoring offers a more reliable and secure path in adHoc network in traffic flow modeling. The validations of the proposed approach were developed following the energy conservation and security provisioning in adHoc network.***

Keywords: Wireless adHoc Network, multi-objective function, energy coding, security routing.

I. INTRODUCTION

The constraint resource and dynamic nature of adHoc network limits offers a constraint in the deployment of adHoc network under various critical applications. The dynamic nature has a impact on the offered security factor and routing performance. The developing approaches illustrates a significant improvement in offering security by different means such as, by building a route monitoring mechanism, by monitoring the packet exchange and blockage factor. Mobility characteristic of nodes is a concern in adHoc network. The possibility of network nodes moving out is very high as each node moves in multiple directions. This results in collapse of communication network. Hence, for the need of communication a method of controlling the flow traffic based on the node property data for optimal route selection is required

As communication mode for long range communication, Adhoc network has become a powerful communication mechanism with non-dependencies in infrastructure, such networks are growing fast.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Ugendhar Addagatla*, Department of C.S.E, Guru Nanak Institutions Technical Campus Ranga Reddy, Telangana, India. ugendhar2008@gmail.com
Dr.V. Janaki Department of C.S.E, Vaagdevi Engineering College Warangal, Telangana, India. janakicse@yahoo.com

While self-generating characteristic has given a high portability in communication with adhoc networks, such networks have limitations on their route and their offering features. Several researches have been made to formulate efficient routing protocol for data exchange in the mobile Adhoc network. Different approaches for route detection in adhoc network and the safety concerns are the evolving issues. While each node is an active member, when communicating as a source or a receiver on the network, reliability of the communication node has an crucial role. Depending on the routing methods in various security approaches, it is observed to ensure per-node protection at node level.

A trust driven security for security provisioning is presented in [1]. The suggested approach defines a new security monitoring factor based on the reliability factor in the routing. In [2], security provisioning the routes based on rules for defining the behavior is suggested. The host based and source based coding is presented in these approaches. ANT based routing is defined in [13]. A pheromone based monitoring is suggested to detect route in adHoc network. The scheme optimizes the route selection based on the node characteristic defined as pheromone. A process for mobile adhoc networks using a bi-simulation method of routing scheme is presented in [4]. In [5], an approach for the design of the network parameter defining method for efficient network design is proposed. The [6] outlines an energy driven AODV protocol called "EN-AODV" for energy routing in adHoc network. It is based on the scope of the data transmitted by the nodes and the received rates, which defines or maintains the energy level. This method is outlined based on the scope of the data transmitted by the nodes and the received rates, which defines or maintains the energy level.

In [7], an anonymous routing protocol based on the location is developed called as protocol (AO2P) is developed. In AO2P links are selected on a random based following random share selection for next hop. A route request is to be forwarded from a source to the destination in this communication. So preserving the location information in this geographic position based routing is quite challenging. So the location has to be preserved such that it should not reveal to the nodes outside the network. [8] Specifies a security protocol called PRISM. This approach develops tracking-resistant mechanics for managing routes in Adhoc network. This approach depends on surrounding environment such as the size of the network and the motion type of a node and defines the offering of security in the network.

The source identification, however in this approach, the location are derived from the GPS unit, and a trusted offline monitoring authority is used for the tracking purpose.

A dedicated off line tracking authority may not be feasible in all real time scenario. Due to the constraint of the method in listing out the nodes reliability the selection is less optimal in approach. To eradicate such problem in [9] a location clocking using geographical routing is proposed. This routing is called as location secure routing (LSR). Due to range constraint the communication is limited with the nodes which are in the radius of communication limiting range. This constraint limit the node interconnects and intern decreases the throughput. The topology of the network keeps changing in such network so nodes in vicinity for communication are not an optimal solution. To avoid such limitation in [10] an admission routing protocol for adHoc network is suggested. In [11] using a similar manner, a key management is introduced for a safe route. Routing rounding ensures successful running data between authentic nodes around the network or existing unfriendly nodes, and ensures the foundation of a secure MANET system. In [12] a Local Service Management Protocol is introduced following a location service management protocol called "MRLSMP". Its objective was to find the observations for installing aligned frameworks to control location information using geographical clustering increased message aggregation. A hybrid features a simple protocol to protect the route formation for data transmission, and ensuring user privacy is outlined in [13] for adHoc network.

The use of a time sessions key increases the relative probability of attacks. To avoid a lightweight protection-protection is presented in [14] in concerning to a source of reliability and routing privacy. This approach minimizes the network overhead, but dynamic key selection leads to a constraint of compatibility. Because the keys are selected dynamically, the key for the non-repeating or security character is not checked. However in [15] to achieve a security factor a threshold cryptography following a decentralized access point controlling is proposed.

Although multiple keying mechanism or authentication schemes were developed, the distribution architecture and the unbalanced use of storage resources are constrained. To overcome such issues in [16] a load balancing approach is suggested. A similar objective in a dynamic condition in the mobility condition for communication protocol is presented in [17] that specify the location of the nodes from positions like GPS. A region-based Location Service Management Protocol (RLSMP) was defined which works to manage location information using a broadband type message aggregation method. Sharing location information based on the node identity broadcast in such code. The vast casting overhead is ignored in such approach.

This distribution guarantees security credibility when identification is shared, but the network route overhead has increased. Reliability networks are credited to a node based on the trustiness factor [18]. By searching for mutual relation and differences in trust in the network, the trust network develops confidence levels and develops trust metrics for each node in the network. The process of reliability based on the content of the data. However, in these approaches there is no security addressed due to geographical location. To obtain the objective of providing an infrastructure free secure routing protocol in [19] security management is achieved by defining an inter-nodal repetitive message for node behavior monitoring. An advanced method called a geographical hash has been suggested for encoding which provides memorable geographical information. It is a broadcasting approach that focuses attention on the security provisioning of the location. In [20] a protocol Called ARAKE is developed to achieve similar goals in an easy-knowing rounding protocol. In this network it is observed that there are also intermediate node where the sender and the receiver are not anonymous, and are defined simultaneously from the network. The approach to route attack is very strong in this case. A conventional approach to identification is identified on a stable node is presented in [21]. In this work, a Demand based Routing Protocol termed MASK is proposed. This communication develops a MAC and network-layer communication on the ad hoc network. However, on run attacks are not defined in this approach. Observing such approach it is likely to be the subject of computational computation when considering two components for protecting the security systems. In [22] TR-Routing based in tree routing is presented for a Ad Hoc Network. This approach is a well defined routing security system that evaluates redundant information, evaluates longer operation, and maximizes network life time and develops a tree coding to achieve long term node activities. In another approach BAN logic [23] is presented. In this presentation, a BAN logic for Authenticated Routing for adHoc Networks (ARAN) with the approach of redundancies effectively. The past development illustrates different format of security approaches for Adhoc network. However, the constraint of offering security is limited to the reliability factor, wherein the network observe a quality deviation in offered service, energy minimization and life time constraint in adHoc network. The issue of offering hence needs to be resolved with the consideration of multiple factors optimization. In this paper new routing approach following multiple monitoring attribute is proposed. To present this paper, the rest of this paper is presented as Section 2 outlines the existing security routing and the proposed conservation approach for security coding using an operation schedule controlling. Section 3 outlines the approach of monitoring multiple factor monitoring and routing scheme proposed. Section 4 outlines the simulation result of the proposed approach. Section 5 concludes the presented paper.

II. SECURED ENERGY CONSERVED ROUTING IN ADHOC NETWORK

For trusted route in adHoc network, a process for optimization operation is needed for network optimization. Network functionality in Adhoc network is more effective, where the observed reliable nodes are defined for power switch to increase node life time. To obtain the objective a 802.11 CSMA/CA protocol following MAC layer is developed where a scheduling scheme following an Active_Masters and link continuity of forwarding the packets to other node called AWAKE is suggested.

In most cases, a link is heard in a schedule period and if the node is not scheduled to transfer or receive data, it will enter to a OFF mode. The wake period are defined as (T_1, T_2), (T_2, T_3) ... (T_n, T) for a link period. Wake up on active cycle for once on a wakeup period. All nodes disallow broadcasting packets (0, T_1) during the broadcast window period. In the initial period (0, T_1) of the link period, all nodes remain simultaneously ON. If there is anything to send or broadcast the node keep a listen request to the node.

The broadcast window for the duration (0, T_1) listen for the packet which cannot be sent in previous attempt is packed at the Mac Layer. This buffer at MAC layer is passed at the end of the broadcast window. On the final stage each node enters to a broadcast period and all nodes wake up at a period T_1. If the node has no packet to transmit or broadcasting it enter to sleep mode. On each wake period, there is an active node on the wake-up cycle. Each node is allocated with a wakeup period of T_w given by,

$$T_w = T_{listen} + T_{comm} \quad (1)$$

Where, T_{listen} is the time for the listening process and T_{comm} is the time taken for communication.

Towards energy conservation, an optimal route is chosen during setup phase of an adhoc communication. In the selection process, each of the possible routes is evaluated with the aggregated energy level. The route with the possible energy level having greater than the required energy level is then chosen. The required energy level for a transmission E_{tx} is defined by,

$$E_{tx} = \frac{P_{sz} \times p_{tx}}{B_L} \quad (2)$$

Where, P_{sz} is the size of the packet of transmit, p_{tx} is the required power for each packet transmission, and B_L is the offered bandwidth for data exchange. The transmission power p_{tx} is depend on the distance required for the data to exchange. The transmission energy is then defined as,

$$E_{tx} = d\ X \frac{P_{sz} \times p_{tx}}{B_L} \quad (3)$$

Where, d is the distance to travel.

In the exchange of data packet the network follows a topology driven communication scheduling protocol, where each of the node is operated on a schedule period of listening and sleep mode according to the type and energy level of each registered node. Each of the nodes in the network is registered to its neighbor node for the energy availability, for a node with higher energy level in the network takes the responsibility of data exchange. This process control the flow of data in a specified link format where the less power nodes called members are scheduled to exchange data in the listening period and the highest energy link node takes the responsibility of data exchange towards the sink. The route scheduling scheme for each node minimizes the energy consumption.

However, the reliability of this route is not been evaluated with respect to the scheduled period of operation and the link energy utilization. In the proposed approach of energy conservation, each of the nodes is constraint with the registration of highest energy link node with two add-on parameters of dynamic energy conservation period and maximization of the residual energy level. The proposed approach select the link route based on the maximization of energy saving period and total residual power. The residual power E_{res} is measured as a energy parameter in the link route selected after each packet exchange. Here, a sub setup period is allocated per communication period, where the nodes undergo the residual power consumption to validate the energy consumption and residual energy for the retention of the route. In the communication process in this approach route is selected which satisfy the constraint of,

$$R_{sel} = \max (E_{agg}) \quad (4)$$

For the selected route then a topology governed data exchange is performed where the mode with the highest energy level is given the responsibility of data exchange and all the nodes with lower energy level is set to listen period for a scheduled period. Wherein conventional approach, the member node sends a request to wake after a schedule period, a non-pending request leads to extra power dissipation, wherein in this approach, the registering node sends a 'ON' signal to the registered node when a communication request is observed. Here each of the nodes is set to power save mode until the registering node sends a request to the registered node. The extension of the power save period leads to higher energy conservation hence giving more route lifetime. The illustration of a extended power saving approach is illustrated in Fig.1.

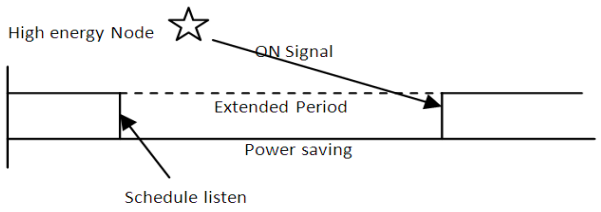

Fig.1: Extended Power saving schedule

The optimal selection of the route with max (E_{agg}) and the extended energy save scheduling leas to higher energy saving and hence leads to a more reliable routing approach in adhoc network. To derive a reliable secure routing approach, in [1], a new routing scheme based on the trustiness factor and residual energy level is proposed. The presented Energy Efficient Secured Reliable Routing Protocol (EESRRP) [1] defines a adaptive threshold calculation and energy model based on a inspect and inspect_ack signal. The methods derive the residual energy level.

All nodes are assumed to be with power detection unit. Transmission power limitation is restricted to achieve high conservation for controlling interaction of the wireless nodes. To achieve a high energy saving goal a linear modeling is developed. The lowest power distribution algorithm is defined as the least energy distribution among the nodes. In a asymmetric link where $N_{i,j} \neq N_{j,i}$, the power allocation is controlled by the allocable data rate K_i. The allocable rate is defined by,

$$\max\left(\sum_{i\in N} K_i\right) \quad (5)$$

Subjected to,

$$\sum_{j\in N_i} K_{ij} - \sum_{j\in N_{i+}} K_{ji} = K_i \quad (6)$$

Here the number of node is N_i, which can approach the external nodes N_{i+i}.

If the symmetrical link condition is present, the nodes communicate with a feedback. In this case the node is 2-way communicated with $C_{ij} = C_{ji}$. In such cases the data packet interaction is defined,

$$\max\left(\sum_{i\in sources} K_i\right) \quad (7)$$

Subjected to,

$$\sum_{j\in N_i}(K_{ij} - K_{ji}) = K_i, \forall i \quad (8)$$

The topology selection of links to satisfying required criteria due to the restriction of permissible power level and data traffic from the selected topology is further controlled. However, the constraint of node dynamic characteristic is not considered. So, the energy control does not give much yield. To better work, the node features of communication are monitored.

These allowed energy controls are traffic conditioned. Therefore, the minimum blockage probability (P_{con}) is monitored to satisfactorily use p_i for network topology, which is likely to be interrupted. However, choosing these paths will become an open loop problem, and sometimes the optimal paths will not achieve. Therefore, the source feedback will be generated to provide access to the route through interface control and search control. The feed data link contains the node block in the node.

In this specific approach, this blockage factor 'f_i' is used as a transfer feedback to prevent extra power dissipation. A rate control factor, D is derived as a function of 'fi' given by,

$$D = (L_{max} - f_i) \quad (9)$$

To obtain better control, every unit operates on limit for a maximum range of two boundaries, so that it may get a high traffic potential flow. In non-linear traffic condition the traffic is randomly varied and the blockage is non-linear which varies at the range of L_{max} to L_{min}.

III. MULTI-OBJECTIVE ROUTING IN ADHOC NETWORK

A multi-objective function is defined in the routing observation of adhoc network. The function is separated from each node as a passive parameter. Precise reception is a node receiving a proper packet when listening to the next hop node ahead, instead of waiting for clear access to each packet via the next node in the route. An Acknowledgment P_ack is used to track the forwarding while transmission. P_ack cannot be used with the last path because it will never restore a packet. P_ack requires two conditions: the nodes are in the way that their network interfaces are unavailable, and network links work bidirectional. P_ack works on the link-layer (IEEE 802.11b) in a two-dimensional array of node.

Here node detects the next node which is in front of its data exchange. When the next node is forwarded, a synchronous acknowledgment (ACK) is generated. If the next packet does not move forward, a negative ACK is generated. Through the P_ack acknowledgment method, the next node can early predict the forwarding success rate of the pact in the communication. To monitor this communication the node needs to govern the operational characteristic of each node. The proposed approach defines a link updation factor in multi objective mode where each node update the node level monitoring for optimal route forwarding. The process is as outlined below.

A) OBSERVING DIRECT EXCHANGE

In this step, each of the nodes observes a direct link exchange of packet. This step gives the forwarding state of the packet by mentoring the acknowledgment developed by a direct access link in the network.

B) UPDATING DIRECT OBSERVATION

The first-link information record is $f_{i,j}$ (ξ, Ω). Initially, it is set (1,1). For every observation, the method updates these factors. On a blockage the weight of the factors obtained in the past is decreased. The updation of these factors is as outlined,

$$\xi := \mu\,\xi + s \quad (10)$$

$$\Omega := \mu\,\Omega + (1-s) \quad (11)$$

the updation factor 'μ' is given as a updation for the past observations made.

$$Fw_{i,j} = Fw_{i,j}(\mu\,\xi, u\,\Omega + 1) \quad (12)$$

For every communication cycle there is a updation given by,

$$\alpha := \mu\,\xi \quad (13)$$

$$\Omega := \mu\,\Omega \quad (14)$$

C) UPDATING NODE RATING

The node i update its first link factor on the acknowledgment it receives. The reliability factor of the nod j, is defined by the two updated factors (ξ', Ω '). This is updated as,

(1) As packets are forwarded.

(2) Observed from the side link nodes.

The updation of the rate factor is given as, $R_{i,j} = r_{i,j}(\mu\,\xi', \mu\,\Omega' + 1)$. The updation is given by,

$$\xi' := \mu\,\alpha' \quad (15)$$

$$\Omega' := \mu\,\Omega' \quad (16)$$

D) DEFINING RELIABILITY FACTOR

Each transmitting node 'i' defines a record for keeping P_ack queue up and setting P_ack timer. When the P_ack timer is off, the next packet is forwarded. In this case, the node observe this as an operation of incorrect behavior through the node j and update the first link information about node 'j' behavior to node 'i'. Each node defines the Reliability factor given by,

$$Fw_{i,j} = Fw_{i,j}(\mu\,\xi' + 1, \mu\,\Omega') \text{ and}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

$$Rl_{i,j}(\xi', \Omega'):= Rl_{i,j}(\mu\ \xi'+1, \mu\ \Omega') \quad (17)$$

E) OBSERVING PATH MONITORING

The algorithm above mentioned gives the complete illustration about the network security evaluation in the view of cost. However, the major drawback with this approach is it does not specify any dynamic conditions of the network i.e. various volatile conditions of network, various structures of network and nobilities of network nodes. The method above mentioned didn't specify any network security evaluation parameters in the regard of dynamicity.

In communication process, each node is scheduled for the time needed in data exchange, which collects data from the centralized buffering node located on the cluster level and passes it to the node. Scheduling approach is an optimal way to adHoc communication for energy conservation. However, nodes are scheduled at the initial stage in a predefined manner. This adds more computing and monitoring energy dissipation in adHoc network. An extended schedule is proposed to avoid this, and where a request is observed, a 'Wake' signal generates a listening signal of a node and an extension in the sleep period is observed.

The process of communication in a cluster based communication is depicted below.

For a successful communication, a route (R_i) is defined as,

$$M \Longrightarrow CH \Longrightarrow GW \Longrightarrow CH \Longrightarrow M$$

Where, M is the member node. The route is then selected based on the constraint,

$$Sel\_Route = \max(\min(\sum I_i)\ P_i) \quad (18)$$

Where, (I_i) is interference observed by the head node from all the linked GW. The operative Pseudo code for the controller unit is outlined as,

```
Process (knock)
Sleep = '1';
        If knock='1' then
        Wake = '1';
        Sleep='0';
        Else
        Wake='0';
        End if;
End process;
```

During the data exchange, for broadcasting from a source node $n \in S_i$ usually an average data rate of $R_n^{(i)} \geq 0$ for $i \in \square_n$ is allocated. To select high-throughput links according to the traffic distribution, the multipath routing comes in a number of ways to reach destination. The traffic source rate in this case is defined as,

$$s \triangleq [S_n^{(i)}]_{n \in S_{ii \in T_n}}, \quad (19)$$

As the input data rate of sources and

$$r \triangleq [r_l^{(i)}]_{l \in \mathscr{L}_{out}(m), n \in N \setminus D_i, i \in T_n} \quad (20)$$

$$\mathscr{L}_{in}^{(i)}(n) \triangleq \{l \in \mathscr{L}_{in}(n) | Tx(l) \notin D_i\} \quad (21)$$

and

$$\mathscr{L}_{out}^{(i)}(n) \triangleq \{l \in \mathscr{L}_{out}(n) | Rx(l) \notin D_i \quad (22)$$

As a set of incoming and outgoing links.

To define a fairness element, each node outgoing (log) gives auxiliary variables for keeping the local copy of the forwarding flow. The data that contains the perfect match of the original is recorded and the difference in information is used in the control of the Lagrange multiplier $\lambda_n^{(i)}$. An optimizing cost function is defined as,

$$\max_{V_n^{(i)} \geq 0} \{\mu_n^{(i)} X_n^{(i)} V_n^{(i)} - \lambda_n^{(i)}[t] V_n^{(i)}\}, n \in V_i \quad (23)$$

Here, the Link optimization is governed by the convergence effort used in maximizing the link cost function based on the r. This function is used to define the fairness Probability of the reputation value V and updation factor μ for a node X in the network.

IV. SIMULATION RESULTS

For evaluation of the offered monitoring parameter a random distribution network is created with each node with a different value. To evaluate the performance of the proposed approach, the approach developed over the 4 simulation scenarios that have been checked for single hop, and multi-hop network, under the random and full sequence search scheme. To observe the performance of the proposed approach a success rate metric is computed. This unit is evaluated for the proposed integrated data traffic model (IDM) with existing EMAC model [15]. The network delay and the transmission success rate are evaluated. The parameter success rate is given as,

$$SR = \frac{\text{No.of packet Succesfully received}}{\text{Total No.of packet generated}} \quad (24)$$

The network parameter used is given in Table 1.

Table 1: Network parameter used

Network Details	Parameters
Node distribution	Random
No. of PU	10
No. of SU	20
Network area	30 x30
Number of channel	10
Communication range	10
Interference margin	0.15
Network variability rate	5

This simulation has been done in two ways. Here the node is retained static and then varied with different node density. Observation of the simulation is outlined below in Fig. 2 for the simulation a network is developed with the nodes deployed in a network area of 30x30.

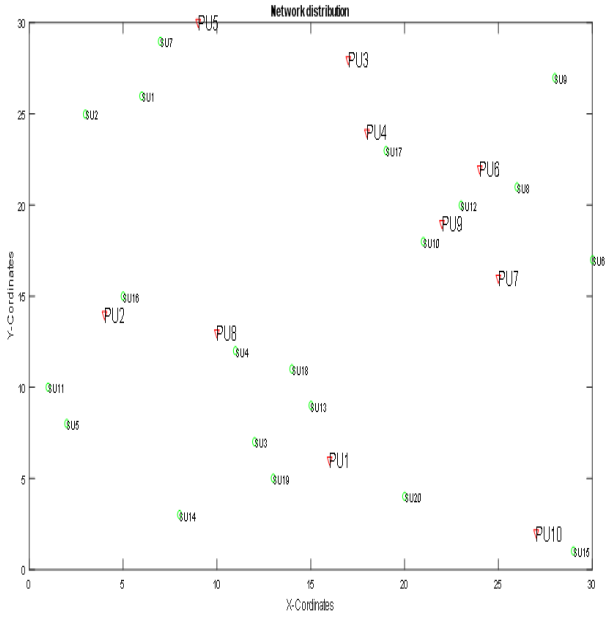

Fig. 2: A 30x30 node distribution

The nodes are randomly scattered with x-y coordinates. The measured success rate and delay is presented in Fig. 3 and Fig. 4 respectively.

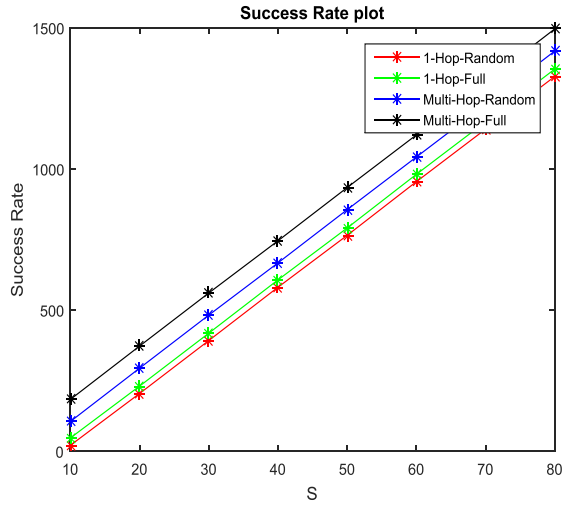

Fig.3: Observation of success rate in the network

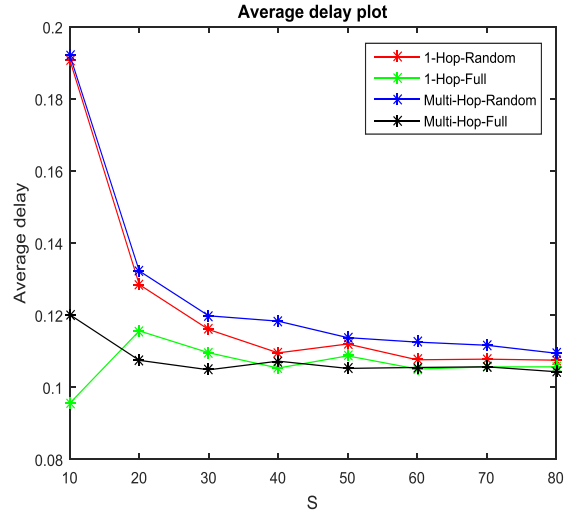

Fig.4: Delay observation of the network

A full search success rate in the multi-hopping data exchange is high as the available slot for data exchange is higher. The delay in this case is observed low. The proposed approach is compared with the EMAC approach applied to the node variation and validated with the parameters. Results shown for the variation in node density is shown below.

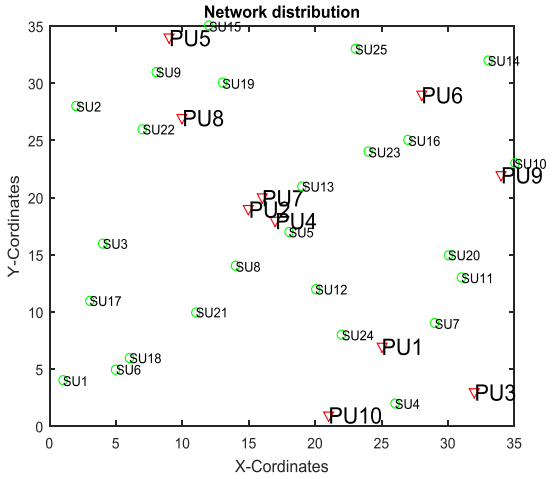

Fig.5: 35x35 node distribution

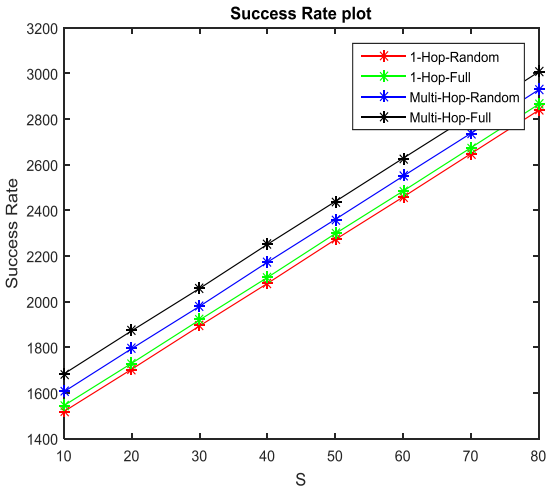

Fig.6: Success rate observation

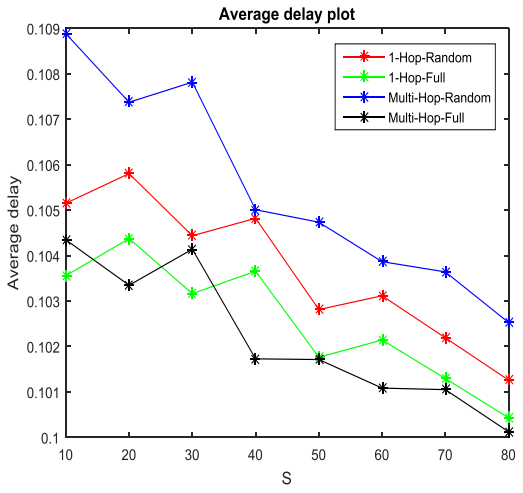

Fig.7: Delay factor observed for 35x35 node density

With the addition of 5 units, 1500 units of success rate enhancement are achieved. The average delays in this case have been cut by a factor of 0.1 seconds. Node density of 10 and 15 is simulated and the observations were as listed below in Fig. 8

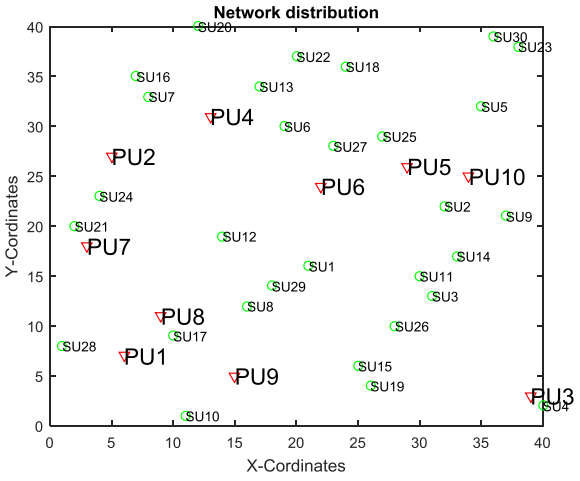

Fig.8: A 40x40 node distribution in the network

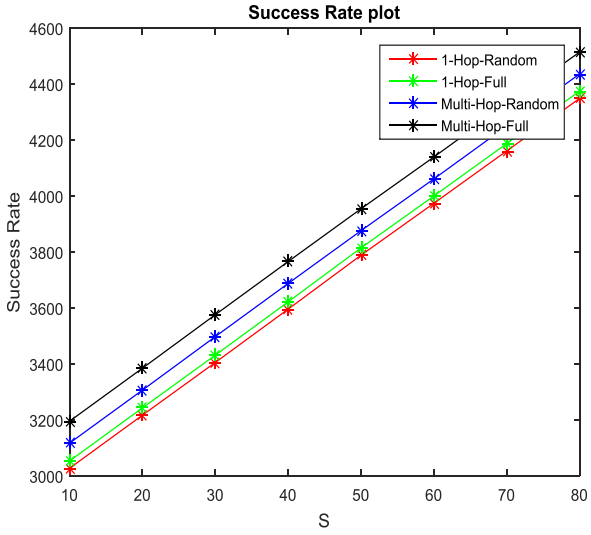

Fig.9: Success rate for 40x40 network using IDM approach

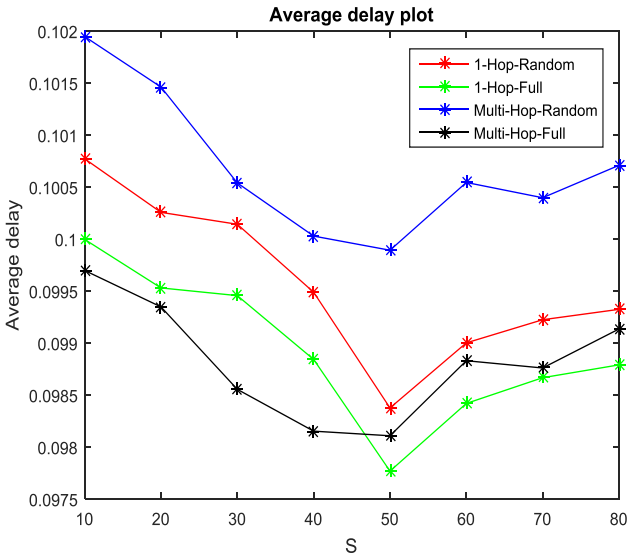

Fig.10: Delay observation over offered slot for IDM approach

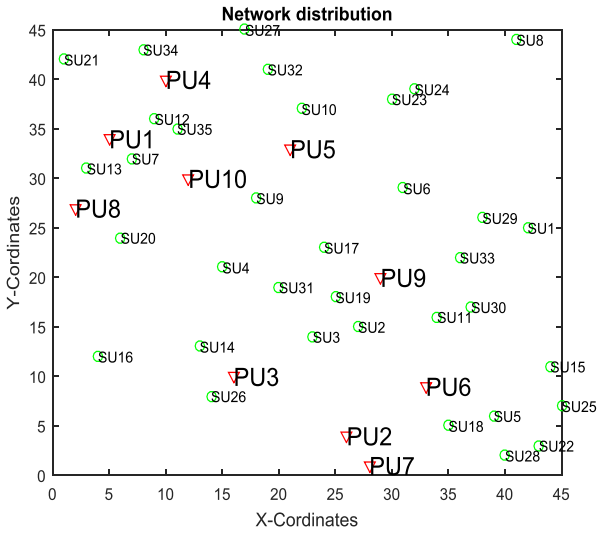

Fig.11: 45x45 Node distributions

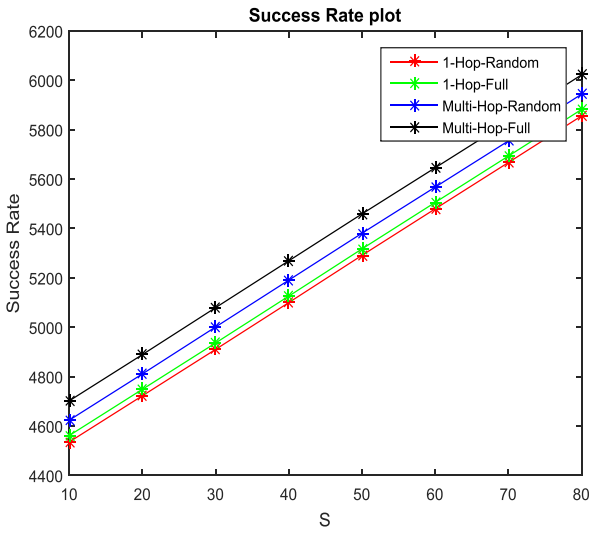

Fig.12: Success rate observation for IDM approach

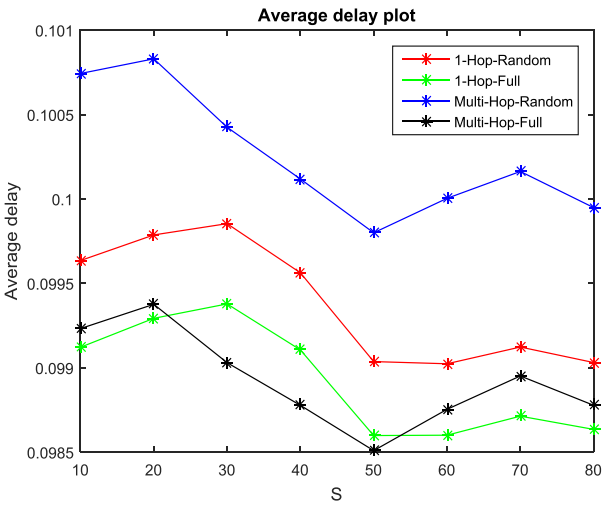

Fig.13: Average delay using IDM approach

A comparative result for the developed approach is given in Table 2.

Table 2: Comparative result for the developed approach

Method	Success rate	Average Delay
EMAC [15]	[7 7 4.5 2.8 0]	[4.3 4.3 7 9.1 11.4]
Proposed IDM approach	[11 11 10.5 10 9]	[4.2 4.24.8 5 6.2]

V. CONCLUSION

Analysis and a communication approach have been suggested for a secure and energy conservation modeling. The approach controls the energy allocation and memory restriction were mortified near the data flow controls. A cross-layer modeling and control of the physical layer and the MAC layer is proposed. The joint control algorithm is applied to each node to consider the power level and trust ratio. A power allocation is governed by using the trust and traffic flow. A multi-objective control operation has been introduced to obtain a higher throughput for the variant traffic condition. The observation illustrates an improvement in success rate and minimization in average delay for adHoc network.

REFERENCES

1. A. B. M. Alim Al Islam, Chowdhury Sayeed Hyder, Humayun Kabir, Mahmuda Naznin, "Stable Sensor Network (SSN): A Dynamic Clustering Technique for Maximizing Stability in Wireless Sensor Networks", scientific research wireless sensor network, 2010.
2. Sandra Sendra, Jaime Lloret, Miguel García and José F. Toledo, "Power saving and energy optimization techniques for Wireless Sensor Networks", Journal of Communications, Sep 2011.
3. SubhashDharDwivedi, Praveen Kaushik, "Energy Efficient Routing Algorithm with sleep scheduling in Wireless Sensor Network", International Journal of Computer Science and Information Technologies, 2012.
4. Alireza Seyedi and Biplab Sikdar, "Modeling and Analysis of Energy Harvesting Nodes in Wireless Sensor Networks", IEEE- 2008.
5. Xenofon Fafoutis, Nicola Dragon, "ODMAC: An On-Demand MAC Protocol for Energy Harvesting - Wireless Sensor Networks", PE-WASUN'11, November, 2011.
6. Alvin C. Valera, "Survey on wakeup scheduling for environmentally-powered wireless sensor networks", Elsevier, 2014.
7. Xiao Lu, Ping Wang, DusitNiyato, and Zhu Han, "Resource Allocation in Wireless Networks with RF Energy Harvesting and Transfer", IEEE Network, Vol. 29, (6), 2015.
8. PrusayonNintanavongsa, M. YousofNaderi, and Kaushik R. Chowdhury, "Medium Access Control Protocol Design for Sensors Powered by Wireless Energy Transfer", IEEE, INFOCOM, 2013.
9. ZhiAngEu, Hwee-Pink Tan, Winston K.G. Seah, "Design and performance analysis of MAC schemes for Wireless Sensor Networks Powered by Ambient Energy Harvesting", ELSEVIER, 6 Aug 2010.
10. D. Li, B.Wang, and X. Jia, "Topology control for throughput optimization in wireless mesh networks," in Proc. 4th Int. Conf. MSN, Dec. 10–12, 2008.
11. Xianren Wu and ZhiTian, "Optimized Data Fusion in Bandwidth and Energy Constrained Sensor Networks", ICASSP,IEEE, 2006
12. M. X. Cheng, X. Gong, and L. Cai, "Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks," IEEE Trans. Wireless Commun., vol. 8, no. 7, pp. 3770–3779, Jul. 2009.
13. K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, "Impact of interference on multi-hop wireless network performance," in Proc. 9th Annu. Int. Conf. MobiCom, 2003, pp. 66–80.
14. J. Tang, G. Xue, C. CLinkler, andW. Zhang, "Link scheduling with power control for throughput enhancement in multihop wireless networks," IEEE Trans. Veh. Technol., Vol. 55, No. 3, pp. 733–742, May 2006.
15. Maggie X. Cheng, Xuan Gong, Lin Cai, and XiaohuaJia, "Cross-Layer Throughput Optimization With Power Control in Sensor Networks", IEEE Transactions on Vehicular Technology, Vol. 60, No. 7, September 2011.
16. Cheng TienEe, Bajcsy, R., "Congestion control and fairness for many-to one routing in sensor networks" In Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, November, 2004.
17. Chonggang W., Sohraby. K., Lawrence. V, Li. B, Hu Y.M., "Priority-based congestion control in wireless sensor networks", IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung, Taiwan, June, 2006.
18. Wan C.Y., Eisenman. S., Campbell A., "CODA: Congestion detection and avoidance in sensor networks, ACM Conference on Embedded Networked Sensor Systems, Los Angeles, CA, USA, November, 2003.
19. Hull.B., Jamieson.K.,Balakrishnan. H., "Mitigating congestion in wireless sensor networks", ACM conference on Embedded Networked Sensor Systems, New York, NY, USA, November, 2004.
20. Rangwala. S., Gummadi. R., Govindan. R., Psounis. K., "Interference aware fair rate control in wireless sensor networks ACM SIGCOMM'06, Pisa, Italy, September, 2006.
21. R. Zhou, L. Liu, S. Yin, A. Luo, X. Chen and S. Wei, "A VLSI Architecture for the Node of Wireless Image Sensor Network," Chinese Journal of Electronics, 2011.
22. Silicon Laboratories Inc, "The Evolution of Wireless Sensor Networks," 2013.
23. J. Liao, B.K. Singh, Mohammed A.S Khalid, K.E. Tepe, "FPGA based wireless sensor node with customizable event-driven architecture," EURASIP Journal on Embedded Systems, 2013.
24. R. Zhou, L. Liu, S. Yin, A. Luo, X. Chen and S. Wei, "A VLSI design of sensor node for wireless image sensor network," IEEE International Symposium on Circuits and Systems, Paris, 2010, pp. 149-152.
25. F. Hutu, A. Khoumeri, G. Villemaud, Jean-Maurie Gorce, "A new wakeup radio architecture for wireless sensor networks," EURASIP Journal on Wirelss Communications and Networking, 2014.
26. Bharath Keshavamurthy, Abhay Narasimha, Asif Ahmad A S and Poornima G, "VLSI implementation of a novel sensor architecture for Industrial Wireless Sensor Networks", IEEE, International Conference on Computational Intelligence and Computing Research, 2016.
27. Halil Yetgin, Kent Tsz Kan Cheung, Mohammed El-Hajjar, and Lajos Hanzo, "A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks" IEEE Communications Surveys & Tutorials, Vol.19, (2), 2017.
28. Shih-Lun Chen, , Min-Chun Tuan, Ho-Yin Lee, and Ting-Lan Lin, "VLSI Implementation of a Cost-Efficient Micro Control Unit With an Asymmetric Encryption for Wireless Body Sensor Networks" , IEEE access, Vol.5,pp-4077-4086, 2017.
29. Jamila Bhar, "A Mac Protocol Implementation for Wireless Sensor Network", Journal of Computer Networks and Communications, Hindawi Publishing, 2015.

AUTHOR PROFILE

Ugendhar Addagatla, presently working as Associate professor in the department of Computer Science and Engineering at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Hyderabad, Telangana State, INDIA. He has 12 years of teaching experience. He is associated with ISTE and CSI as life member. He has obtained B. Tech. degree in Computer Science and Engineering from Christu Jyothi Institute of Technology and Science, Warangal, Jawaharlal Nehru Technological University Hyderabad, in 2003, M.Tech. degree in Software Engineering from Ramappa Engineering College, Warangal, Jawaharlal Nehru Technological University Hyderabad, in 2008 and my area of Research interest is Mobile Computing, Ph.D (CSE) from Jawaharlal Nehru Technological University, Hyderabad and it is my part of Research work.

Dr. V. Janaki, received Ph.D degree from J.N.T. University Hyderabad, India in 2009 and M.Tech degree from R.E.C Warangal, Andhra Pradesh, India in 1988. She is currently working as Head and Professor of CSE, Vaagdevi Engineering College, Warangal, India. She has been awarded Ph.D for her research work done on Hill Cipher. Her main research interest includes Network security, Mobile Adhoc Networks and Artificial Intelligence. She has been involved in the organization as a chief member for various conferences and workshops. She published more than 50 research papers in National and International journals and conferences. She is presently supervising nearly 10 scholars for their research.