International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

ENERGY EFFICIENT ADAPTIVE ROUTING PROTOCOL TO IMPROVE TRAFFIC CONTROL SYSTEM FOR PAYMENT AND TRUST NETWORKS

Yamini devlal [1], Richa Sharma[2]

[1]M.Tech student of Department of electronics and communication,ABES,GHAZIABAD ,NCR,INDIA

[2] Assistant professor,Department of Electronics and Communication,ABES,GHAZIABAD,NCR,INDIA

Abstract: *The payment framework rewards the hubs that hand-off others' packets and charges those that send parcels. The trust framework assesses the hubs' capability and unwavering quality in handing-off parcels as far as multi-dimensional trust values. The trust qualities is the degree of belief about the hub's behavior which is done by calculating trust values of hub's past behavior and which helps in predicting future behavior. This system can be implemented for sharing data and multimedia data transmission.*

The basic goals of research in wireless sensor network is to enhance the lifetime of the network and also to use the power of the network nodes efficiently which is shown by the proposed routing protocol in terms of consuming energy .The proposed routing protocol depends on enhancement of AODV and by using responsive geographic routing .

Keywords: **WSN, Trust networks, AODV, RREQ, payment systems**

I. INTRODUCTION

The system ought to have the subsequent self-arranging capacity characteristics since the areas of specific hubs are not known toward the forward. The primary quality of this system is the joint effort among the hubs. A huge amount of hubs are used to generate a sensor network and these nodes are arranged compactly to each other to examine them. The data is composed by the every node and transmits that information back to the sink .the hubs are typically autonomous and have different energy capabilities.

The noteworthy application regions of the sensor systems are in military ranges, wellbeing and in normal cataclysm. Likewise, this system is utilized to inspect the light, warmth, dampness and other ecological variables for the social applications. [1] Wireless sensor systems have the consequent attributes:

- It comprises of sensor hubs with some level of vitality which can predict their remaining energy and have the comparative design and One Base Station (BS) without vitality requirement is removed far from the region of sensor hubs.
- All sensor hubs are stationary. They utilize the straight communication or multi-bounce communication to speak with the BS.

- Sensor hubs sense air at a settled rate and at consistent times have information to transmit to the BS.
- The lifespan of WSN is the aggregate sum of time before the primary sensor hub comes up short on power. [2]

With a specific end goal to meet the necessity of stretching out lifetime is to propose vitality proficient routing algorithms that benefits the objective to adjust the heap in the midst of the sensor hubs in the system

This proposed framework defeats these disadvantages by the accompanying strategies, trust and payment framework. The payment framework utilizes credits to charge the hubs that send parcels and compensate those transferring packets [4]. The trust framework is crucial to evaluate the hubs' dependability and unwavering quality in handing-off packets. A hub's trust worth is characterized as the level of conviction about the hub's conduct. The trust qualities are figured from the hubs' past practices and used to anticipate their future behavior. So that the reliability of the route can be predicted

II. BACKGROUND OF THE PROBLEM

Essentially WSN is mobile hubs accumulation, which speaks with different hubs by TV. In Mobile specially appointed systems, they don't have any focal organization and existing base [5]. In this way, the WSN is utilizing a provisional system communication. WSN is working without foundation, so hubs in wireless system progressively frame their own particular system and association on the flying development. In wireless communication all hubs can listen to the communication on the off chance that it is in sending range [6]. These wireless system hubs utilize some default routing protocols to distinguish the sender and recipient for each message. In wireless mobile specially appointed system security is a noteworthy issue, especially in military application.

Officially different methodologies have proposed to handle this security issue [7]. Be that as it may, now there is no routing algorithm is suitable for the situations. Over a few years, more number of systems has been proposed with onion routing method and a few systems have been executed.

III. RELATED WORK

Related studies are as follows:

Reputation-based schemes [8] experience the ill effects of false allegations where some genuine hubs are dishonestly recognized as vindictive. This is on the grounds that the hubs that drop packets briefly, e.g., because of blockage, might be dishonestly distinguished as vindictive by its neighbors. Selfish node behavior degrade the systems performance.. With a specific end goal to decrease the false allegations, the plans ought to utilize tolerant limits to ensure that a hub's packet dropping rate can just achieve the edge if the hub is malicious.

In [9], payment is utilized to give credits for the selfless behavior of nodes by rewarding them and they can use the credit for forwarding their own benefits . A notoriety framework is additionally used to recognize the silly parcel dropping assailants once their packet dropping rates surpass a threshold.

For the proxy discovery, Luo [10] proposed two algorithms eager and on-interest proxy disclosure algorithms. When all is said in done, the covetous proxy revelation protocol is proactive and the on-interest proxy disclosure protocol is latent. The ravenous proxy revelation requires an insatiable way to achieve an proxy customer with high HDR downlink channel rate. An insatiable way is built by a mobile customer sending the course ask for message (RTREQ) to its neighbor customer with the best HDR downlink channel rate for every hop. In any case, this avaricious way may not generally find the proxy customer with the best general channel rate for the destination customer.

IV. PROPOSED METHODOLOGY

a. Experimental Design:

A parallel event driven simulator, Matlab was utilized for comparing the results of protocols. Simulation experiments were run on computer installed with Matlab with impacts of speed of simulation and network size on the trial results energy consumed parameter is calculated. [11]

1)Energy consumed: Energy consumed for control packets made for routing.

Energy consumed were measured for speed of simulation in experiment as provided below using GUI of MATLAB , The underline reality to this protocol is that it surges a course demand message in the system to set up a course and it comprises of two techniques: Route Discovery and Route Maintenance Constant bit rate generator was used for generating packets of fixed size. [12] Three different types of traffic load were used for simulation such as

1. High traffic load – one packet every 0.1 second,
2. Medium traffic load – one packet every second and
3. Low traffic load – one packet transmitted every 10 seconds.

b. Proposed implementation

Our main contribution is to provide a solution for the uniform energy consumption for all the nodes in order to increase network lifetime.

The trust model represents how to calculate the trust of the routing path by using the trust value of individual nodes. Our trust model creates relationship between trust metrics and network statistics. [13]

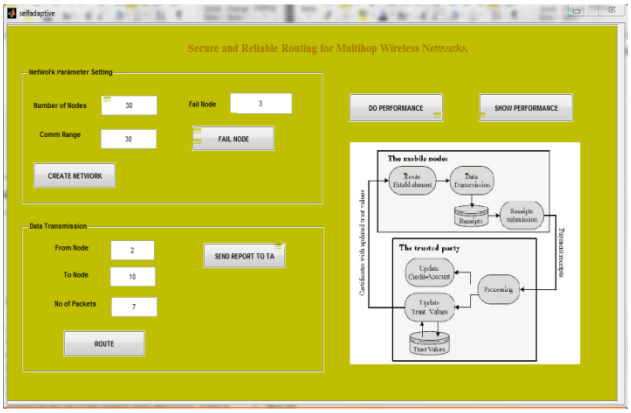

Fig.1: GUI for implementation process

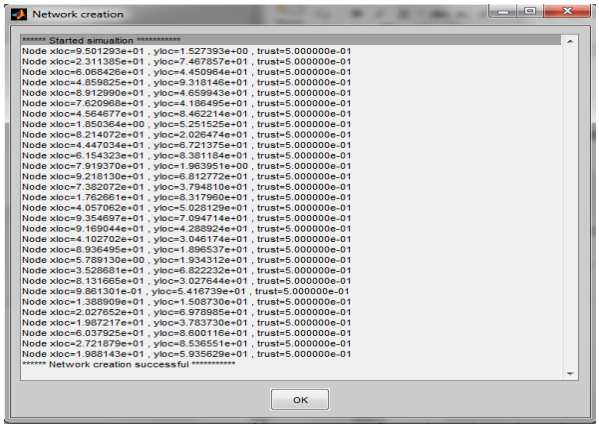

Fig.2: Network created through simulation [14]

Total number of nodes: 30, Communication range: 30

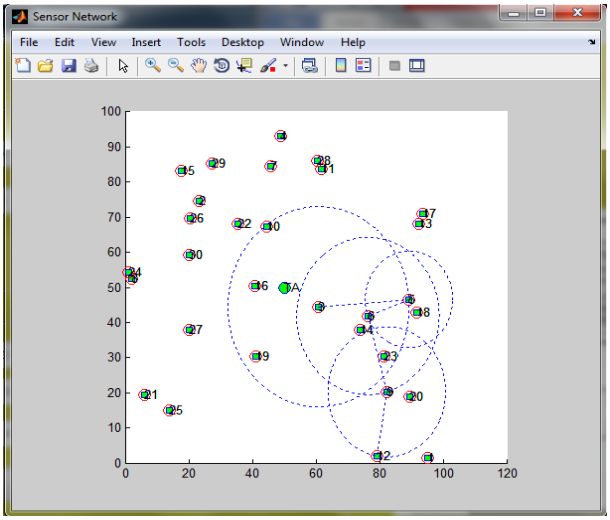

Fig.3: Transmission route network

Sender node: 3 Destination node: 12

The next hop is 2: sending packet to 2, Recieved packet at 2

The next hop is 7: sending packet to 7, Recieved packet at 7

The next hop is 4: sending packet to 4, Recieved packet at 4

The next hop 10: sending packet to10, Recieved packet at 10

The next hop is 3: sending packet to 3, Recieved packet at 3

The next hop is 5: sending packet to 5, Recieved packet at 5

The next hop is 6: sending packet to 6, Recieved packet at 6

The next hop is 9: sending packet to 9, Recieved packet at 9

The next hop is 1: sending packet to 1, Recieved packet at 1

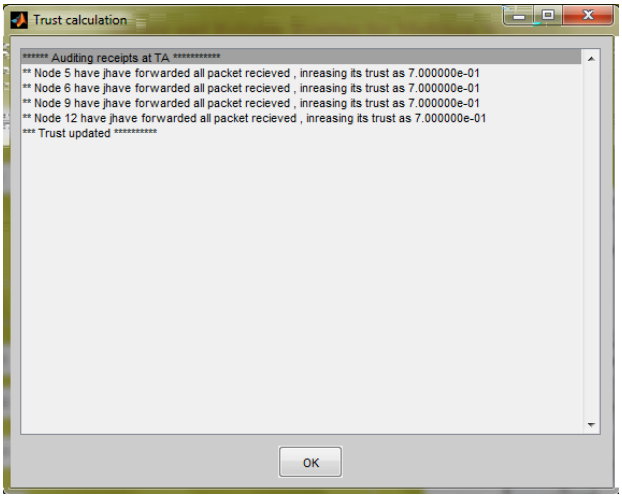

Fig.4: Trust algorithm and auditing receipts at trust authority

Auditing receipts at TA

Node 1 have dropped 23 packet, reducing its trust as 3.000000e-01

Message: Trust updated

V. SIMULATION RESULTS

Simulation results have shown the proficiency of developed proposed protocol for sensor systems applying distinctive routing techniques..

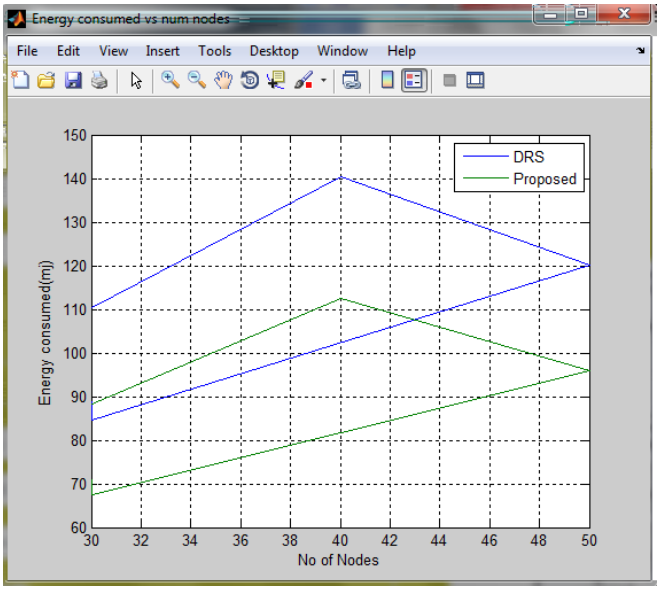

Fig.5: Comparison graph for energy consumed vs. number of nodes

The above fig.5 displayed the correlation results among DRS and proposed routing protocols for energy consumed versus number of nodes in simulation. The Result shows that In this we got the amplified proposed has energy consumed by 11 less by

Table I: Comparison results between two protocols based on different parameters

Parameters	DRS	Proposed
Energy consumed	89.000000	71.200000

VI. CONCLUSION

In proposed framework we utilize onion routing protocol for secure and solid parcel transmission. Proposed protocol gives the layer of encryption and unscrambling procedure to secure the packet while transmitting to destination hub and this framework utilizes the multi bounce course sending algorithm to locate the briefest way from source to destination. Proposed protocol with Advanced Encryption Standard algorithm is a two key encryption process.

Moreover, instruments like data transmission estimation can likewise be incorporated with our way to deal with enhance system execution in mobile specially appointed systems. In future work give security to every packet, so that the gatecrashers can't ready to get or harm the parcels.

VII. REFERENCES

[1] T. Chen, O. Mehani and R. Boreli, "Trusted routing for VANET," in *Proc. International Conference on Intelligent Transport Systems Telecommunications*, October 20-22, 2009, pp. 647-652.

[2] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. International Symposium and Parallel and Distributed Processing*, April 25-29, 2006.

[3] M. Deno and T. Sun, "Probabilistic trust management in pervasive computing," in *Proc. International Conference on Embedded and Ubiquitous Computing*, 17-20 December 2008, vol. 2, pp. 610-615.

[4] T. Raisinghani and S. Iyer, "Cross-layer design optimizations in wireless protocol stacks," *Computer Communications*, vol. 27, no. 4, pp. 213-217, 2006.

[5] M. Satyanarayanan, "Mobile computing: The next decade," in *Proc. 1st ACM Workshop on Mobile Cloud Computing and Services: Social Networks and Beyond (MCS)*, 2010, pp. 5:1-5:6.

[6] S. Khan *et al.*, "Cross-layer optimization for wireless video streaming performance and cost," presented at

International Conference on Multimedia and Expo, Amsterdam, July 2005.

[7] T. Zia, "Reputation-based trust management in wireless sensor networks," in *Proc. International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, December 15-18, 2008, pp. 163-166.

[8] A. Gohari and V. Rodoplu, "Congestion-aware spatial routing in hybrid high-mobility wireless multihop networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 11, pp. 2247-2260, 2013.

[9] H. Luo, R. Ramjee, P. Sinha, L.E. Li, S. Lu, 2003 || UCAN: a unified cellular and ad-hoc network architecture —, in: Proceedings of ACM MOBICOM'03, San Diego, CA, USA, 14–19 September 2003, pp. 353–367.

[10] H. Luo, R. Ramjee, R. Sicha, L. Li, S. Lu,,2003, — UCAN: A Unified Cellular And Ad-Hoc Network Architecture‖, in: The Proceedings of Mobicom, September 2003.

[11] M. Mahmaud *et al*., "Secure and reliable routing protocols for heterogeneous multihop wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, pp. 1-11, 2013.

[12] K. Rana and M. Zaveri, "Techniques for Efficient Routing in Wireless Sensor network," presented at International Conference on Intelligent Systems and Data Processing, 2011.

[13] A. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile Ad Hoc networks," in *Proc. 15th International Conference on Computer Modelling and Simulation (UKSim)*, 2013, pp. 693-698.