ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

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

YAMINI DEVLAL[1] , MS. RICHA SHARMA[2]

Abstract: **The payment framework compensates 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 are appended to the hubs' open key endorsements to be utilized as a part of settling on routing decisions.**

We build up a mobile routing protocol to direct activity through those very trusted hubs having adequate vitality to minimize the likelihood of breaking the course. The proposed routing protocol depends on AODV. Yet, the multifaceted nature is high since security parameters conveyed in RREQ is telecasted and more vitality is devoured. So we will utilize responsive geographic routing protocol to diminish the unpredictability and decrease vitality utilization.

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

I. INTRODUCTION

The system ought to have the self-arranging capacity 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. An accumulation of hubs coordinates keeping in mind the end goal to distribute the gathered data to their neighbor clients in this system. 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 comprise of sensor hubs with some level of vitality can keenness their own particular remaining vitality 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.
- Sensor hubs can alter the transmission vitality of wireless transmitter on the premise of the separation.
- 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 incorporate the objective to adjust the heap in the midst of the sensor hubs in the system. At the point when the workload of a hub is the comparable as that of further hubs, then the remaining vitality of every

All Rights Reserved © 2016 IJSETR

hub will decrease at the comparable rate with system capacity. [3]

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.

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. 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 frustrate the balanced packet dropping assaults, where the assailants drop parcels since they don't profit by transferring packets. 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 et al. [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. Mean end-to-end delay, packet delivery rate and

All Rights Reserved © 2016 IJSETR

routing overhead as measured by the amount of control packets made for routing are the performance networks that were used to consider the two routing protocols. [11]

1. Packet delivery rate: Ratio of packets viably transported to the end to the total number of packets transmitted by the source hub.
2. Mean end-to-end delay: Average time taken for a packet to take off from source to end of the line including course securing deferral.
3. Energy consumed: Energy consumed for control packets made for routing.

Speed of simulation, network size and delay variance are the three control parameters used for this simulation. Packet delivery rate, mean end-to-end delay and energy consumed were measured for speed of simulation in experiment 1 and network size were for three different levels of packet delivery in experiment 2. 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]

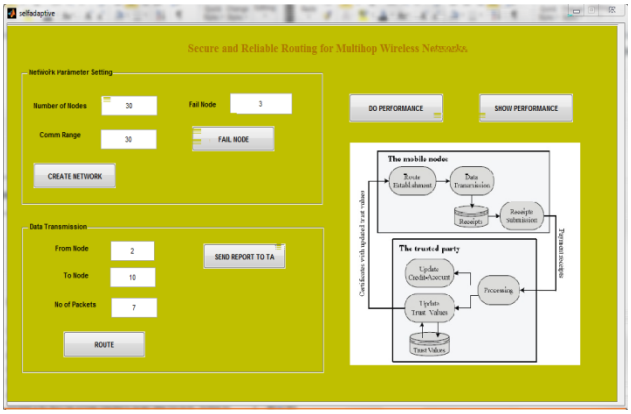

Fig.1: GUI for implementation process

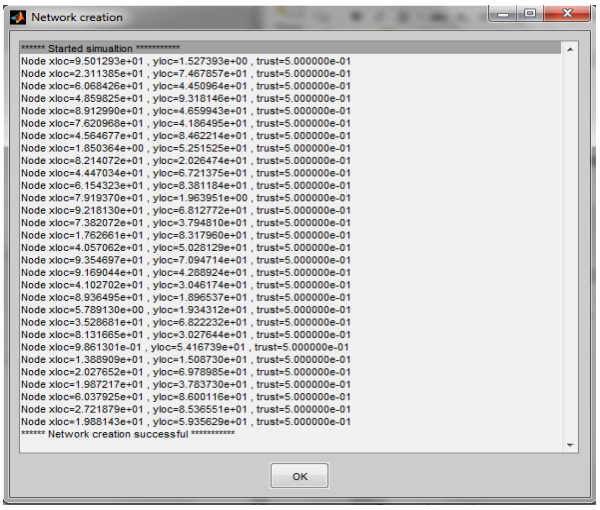

Fig.2: Network created through simulation [14]

Total number of nodes: 30, Communication range: 30

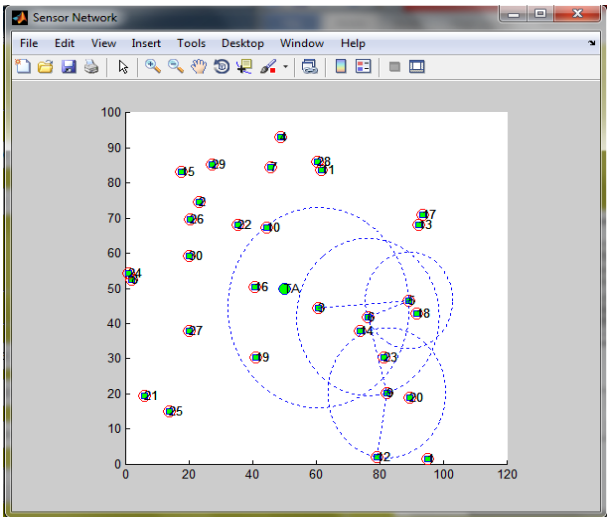

Fig.3: Transmission route network

All Rights Reserved © 2016 IJSETR

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

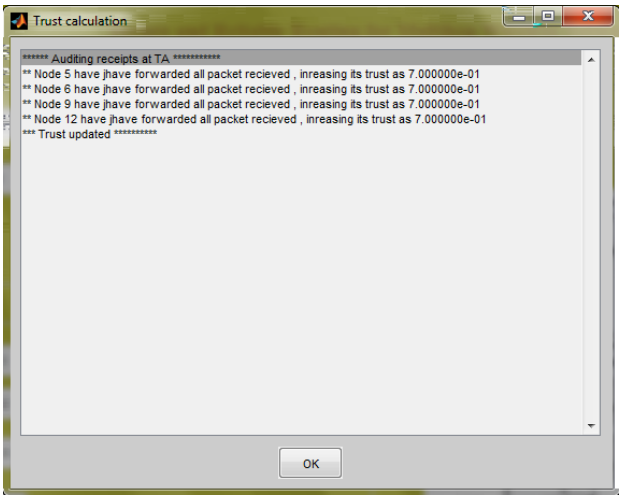

Fig.4: Trust algorithm and auditing receipts at trust authority

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.

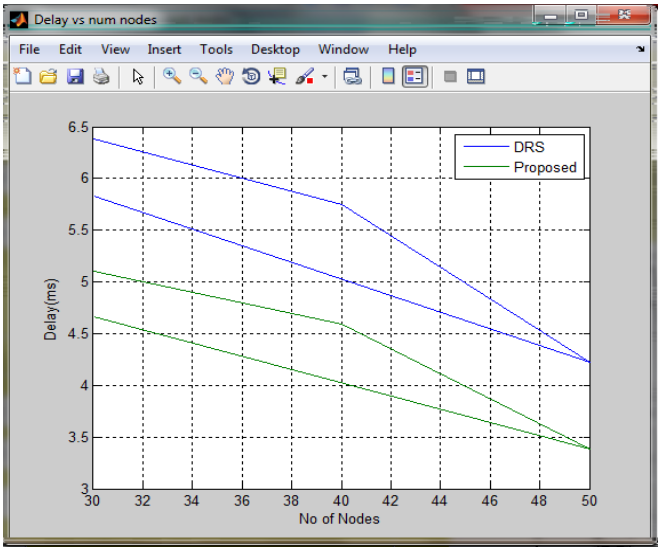

Fig.5: Comparison graph for packet delay vs. number of nodes

The above fig.1 displayed the correlation results among DRS and proposed routing protocols for Packet delay versus number of nodes in simulation. In this we got the amplified proposed has packet delay by almost twice less by DRS.

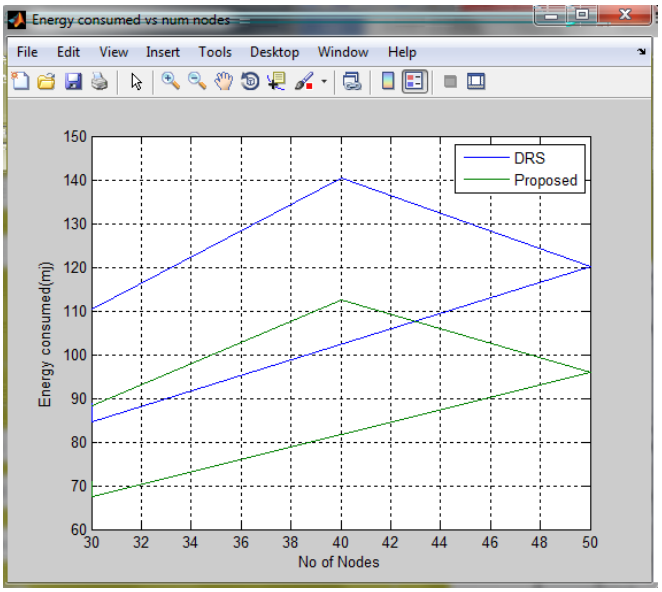

Fig.6: Comparison graph for energy consumed vs. number of nodes

The above fig.2 displayed the correlation results among DRS and proposed routing protocols for energy consumed versus number of nodes in simulation. In this we

All Rights Reserved © 2016 IJSETR

got the amplified proposed has energy consumed by 11 less by DRS.

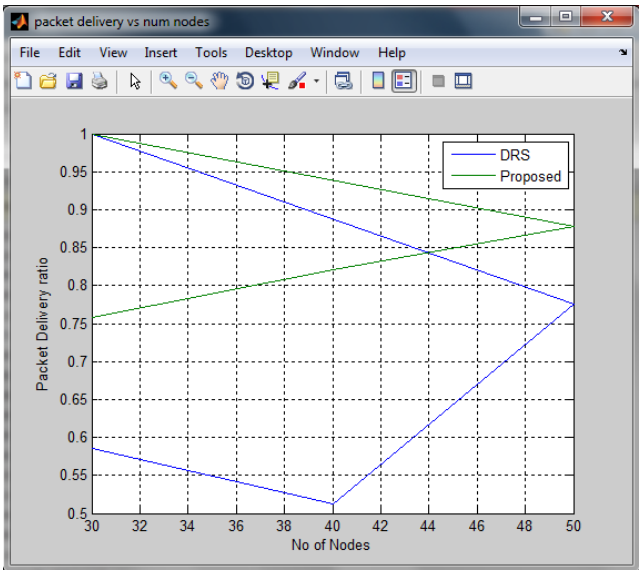

Fig.7: Comparison graph for Packet delivery ratio vs. network size

The above fig.1 displayed the correlation results among DRS and proposed routing protocols for Packet delivery ratio versus number of nodes in simulation. In this we got the amplified proposed has packet delivery ratio by 0.2 more than DRS. The simulation demonstrates that in various circumstances this updating of DRS, we proposed a more productive protocol.

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

Parameters	DRS	Proposed
Packet Delivery ratio	1.000000	1.200000
Energy consumed	89.000000	71.200000
Delay	6.137931	4.910345

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] 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.

[2] R. Shaikh, H. Jameel, and H. Lee, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698-1712, 2009.

[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,"

All Rights Reserved © 2016 IJSETR

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

[7] Kun wang; Meng Wu; Subin Shen,"a trust Evaluation method for node cooperation in mobile Adhoc networks"7-9 april2008

[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] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc On-Demand Distance Vector (AODV) routing," *Mobile Adhoc Networking Working Group Internet draft*, vol. 5, no. 2, pp. 32-34, July 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.

All Rights Reserved © 2016 IJSETR