ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Trust Establishment in Wireless Sensor Network and Forwarding of Packets Using Airport Problem Based Game Theory

J.Angel[1] , T.Ramesh[2]

Research Scholar, Department of Information Technology, Bharathiar University, Coimbatore, Tamilnadu, India[1]

Assistant Professor, Department of Information Technology, Bharathiar University, Coimbatore, Tamilnadu, India[2]

ABSTRACT: Wireless Sensor Networks (WSNs) is a network that has become an ideal area of research in recent years, due to vast potential of sensor networks to enable applications that connect the physical world to the virtual world. A wireless sensor network is a collection of nodes organized into a cooperative network. Trust plays the major role in this research work. In this proposed work first the shortest path of the sensor network is chosen and the packets are sent. While sending the packets, if any of the packets get lost or if the selfish node is identified then automatically it will choose an another shortest part and starts sending the packets meanwhile the distracted node gets isolated so the transmission cannot takes place with the particular node, since the node gets isolated and the packets are send directly to the destination if the cooperation occurs. So In this, the term cooperation takes place among nodes, in such cases the airport problem is the best solution for the transmission of packet among nodes so the trust will be established among nodes.

KEYWORDS : Wireless Sensor Network, Trust, Selfish Nodes, Cooperation game theory, Airport Problem.

I. INTRODUCTION

A Networkconsists of two or more entities or objects sharing resources and information. Computer networks consist of two or more computers that are connected and able to communicate with each other nodes. Networked computers are used to share resources and information. The hierarchy of data should be used in network planning. Wireless Sensor Networks is a network that has become an ideal area of research in recent years, due to vast potential of sensor networks to enable applications that connect the physical world to the virtual world. Each node consists of processing capability and it may contain multiple types of memory.

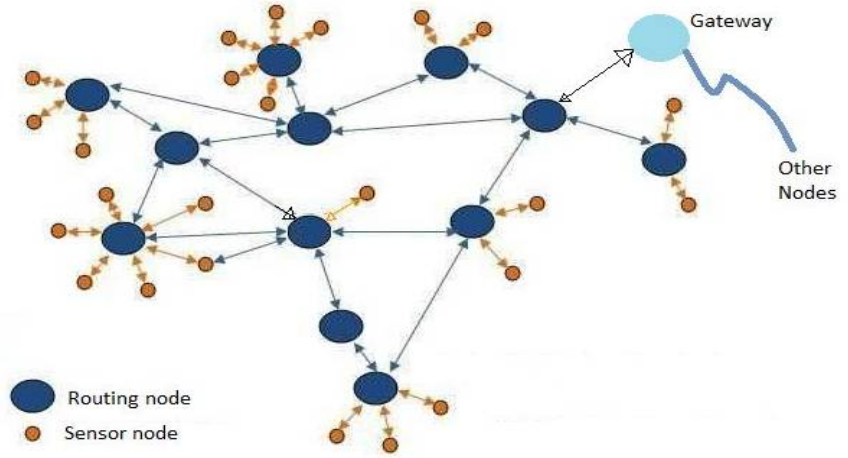

Fig.1.1 Wireless Sensor Network

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

In Fig.1.1 it shows the communication between routing nodes and sensor nodes and this is Wireless sensor networks. In computerscience and telecommunications, wireless sensor networks are an active research area. The impact of wireless sensor networks on day to day life can be preferably compared to what Internet has done. In this it is set up that trust strategy game model, which reflects the gains and losses of the involved nodes. TRUST is the main concept that has to be achieved in this research work. Trust changes dynamically according to the behavior of users. Every user has a particular trust evaluation towards others at a certain point of time or during a certain period of time. Trust value will change as the result of interactions between users. In this research trust is carried out with the help of some coalitional games in game theory.

II. PROBLEM DEFINITION

In this proposed work trust establishment is used and for finding the secure and a trustful routing by means of selecting a cooperative game theoretic strategy, a perfect game theory is used so that the energy consumption and its all performance evaluation meets its satisfactory results and it makes the network performance more reliable.. The concept of Trust in a trust mechanism is common in WSNs, and cooperation between the nodes is based on the Trust concept. Studies on the trust strategy among nodes and trust evolution process of WSN nodes address an important part of trust, and they play a significant role in the stability, security and safety of WSNs.

From the perspective of a single node in a WSN, Trust can promote coordination among the nodes and reduce the risk when cooperating with other nodes. From the perspective of the whole WSN, trust evolves through trust among nodes and improves the cooperation among the nodes as much as possible, following a trust strategy that is based on the allocation of packets and the cooperation of the nodes. The system could reach a stable state and maintain normal communication in the network.

Game theory as a mathematical theory tool focuses mainly on the competitive and cooperative relationship of the participants, and it has been widely used in the field of WSN security. Among various methods of game theory, the airport problem game takes the changing trend of the overall trust as the research object, where sensor nodes of WSNs are viewed as an individual.

III. RELATED WORK

3.1 A CREDIBLE BAYESIAN-BASED TRUST MANAGEMENT SCHEME FOR WIRELESS SENSOR NETWORKS

RenjianFeng, Xiaona Han, Qiang Liu, and Ning Yu proposed a paper in which a credible Bayesian-based trust management scheme (BTMS)[23]is proposed. The overall trust value is aggregated by both direct and indirect trust information. The former is calculated by a modified Bayesian equation and updated by a sliding window. The latter is computed by recommendations from a third party. Moreover, the indirect trust computation is invoked conditionally according to the uncertainty of direct trust calculated via Entropy Theory and malicious feedbacks are excluded. Meanwhile, different recommendations are appropriately weighted in light of the trust levels of recommenders. Simulations are conducted and the results show that, compared with existing approaches, the proposed trust model performs better in defeating attacks.

3.2 EVOLUTIONARY GAME-BASED TRUST STRATEGY ADJUSTMENT AMONG NODES IN WIRELESS SENSOR NETWORKS

Yuanjie Li, HongyunXu, Qiying Cao, Zichuan Li, and ShigenShen have constructed an evolutionary game-based trust strategy model[39] among the nodes in WSNs, and we subsequently introduce a strategy adjustment mechanism into the process of game evolution to make up for the deficiency that the replicator dynamic model cannot reflect the requirement of individual strategy adjustments. Afterward, we derive theorems and inferences in terms of the evolutionary stable state through dynamic analyses, providing a theoretical basis for WSN trust management. Furthermore, we verify the theorems and inferences with different parameter values, especially the trust incentive and the upper limit of data retransmission after packets are lost, and both of them are closely related to the evolutionary stable state.

WSNs have developed from a promising research area to a useful technology that is applicable to real-world scenarios. The applications of WSNs are military applications, environmental applications, health applications, home

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

applications, and other commercial applications. In the near future, WSNs that are comprised of small-size, low-power sensor nodes will become an integral part of lives. Similar to any computer-related environment, security in WSNs is considered to be non-functional but an essential requirement that keeps the complex system available and reliable.

The existing system has proposed Evolutionary Game-Based Trust Strategy. In recent years, in addition to the technology, trust-based security mechanisms have gradually attracted more attention from academia and industry.

Considering the sensor nodes' data retransmission after packets are lost, Trust strategy game model is build and a trust incentive mechanism to promote nodes to choose the trust strategy is also introduced.

The disadvantages of the existing system is that it has mainly focused on the number of nodes (i.e) population of the nodes and it has loss of packets during transmission from one sensor node to other. It also consume very high amount of Energy consumption. It is significant to concentrate on throughput, packet delivery ratio, energy consumption. So this chapter will describe in detail about how those network parameters are solved functionality of the proposed game theory algorithm.

IV. PROPOSED METHOD

In this proposed simulation work trust establishment is used and for finding the secure and a trustful routing by means of selecting a cooperative game theoretic strategy, a perfect game theory is used so that the energy consumption and its all performance evaluation meets its satisfactory results and it makes the network performance more reliable.

When the packet is send by choosing the shortest route from the sensor network and made to send in such a way that the nodes sends the packet from one node to other one by one to reach the destination in such cases, Some nodes will never exchange or give that packets to other nodes and such nodes are termed as Selfish node. In order to save the its energy, the particular node will never send its packet to others.

Assume an threshold value as 0.5. So that when a packet is send from one node to other then each node receives the threshold as 0.5. The nodes are given a rating based on the nodes behaviour. And if the rating is above 0.5, then it is considered as un trusted node or Selfish node. Because it has the rating of maximum so it is considered as Selfish node. But as soon as the selfish node is detected then the selfish node gets isolated. So it will not disturb the entire network often.

The transmission among the nodes is based on how the game plays. Nodes gets its equal share by allocating the equal number of packets among the nodes so that it has to take the given amount of packets to the destination at a given time to its given destination and when the shapley value is calculated then the given number of packets must be equal to its shapley value. Such a way the transmission of packets sent successfully so the trust among nodes is established.

Such a way the selfish node gets isolated and establishes trust to send the packets from the source to the destination.

V. PSEUDOCODE

There are few steps to describe the work and its pseudocode is explained below:
Step 1 : Selecting the Shortest Route
Step 2 : Detecting the Selfish Node
Step 3 : Packets send from the source to Dectination
Step 4 : Trust Established.

Source Node= S, NAmax= maximum value of transmission numbers in the period , Destination Node= D, Trusted Node = TN, Shortest Route = SR, Q = Queuing of Nodes

// Detecting the Selfish Node

```
Selfish_node_detection( NAmax , NAi )
for( each joined node N k in G )
        if (NAmax- NAi< Threshold)
                {
                N k = non-selfish node;
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

```
                }
        else
                N k = selfish node;
        if(NAj= = 0)
                {
                N k is fully selfish node;
                }
}
```

// Selecting the Shortest Route

```
dist[s]'←0
forall'v'∈'V–{s}
        'do"dist[v]'←∞'
                S←Ø
                Q←V
while'Q'≠Ø
        do   u'← mindistance(Q,dist)
                S←S∪{u}
For all'v'∈'neighbors[u]
        do
                if 'dist[v]'>'dist[u]'+'w(u,'v)'
        then
                d[v]'←d[u]'+'w(u,'v)
return'dist
```

//Packet send from source to destination

```
Forward Fromsource()
                If(SR==1)
        then
                {
                beginForward←n
                result:= S→D
                if(result:=cooperative)
        then
                {
                Return←true;
                Packets sent successfully;
                }
        Else
                {
                (SN==1)
//Selfish node detected
        Return←false;
//SN gets isolated
        }
        Else{
                (SR==2)
                Return←true
//Trust Established
                {
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

End If
}}

VI. SIMULATION BACKGROUND

Network Simulator (Version 2), widely known as NS2, is an event- driven simulation tool that is useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989.

NS2 provides users with executable command ns which takes on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation.NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl).. It is mainly intended as a companion animator to the ns simulator.

Linux is one of popular version of UNIX operating System. Linux was designed considering UNIX compatibility. Its functionality list is quite similar to that of UNIX.

Tcl is flexible enough to be used in almost any application imaginable, it does excel in a few key areas, including: automated interaction with external programs, embedding as a library into application programs, language design, and general scripting.

VII. PERFORMANCE EVALUATION

Here the evaluation metrics which have been simulated are as follows:

- Energy Consumption
- Packet Delay
- Packet Delivery Ratio
- Throughput

ENERGY CONSUMPTION

Traffic Rate	ET (Existing)	APT (Proposed)
0.1	3.556	3.323
0.2	3.687	3.459
0.3	3.992	3.754
0.4	4.312	3.991
0.5	4.657	4.340

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Table 7.1 Differences between the Energy Consumed in Existing And Proposed Method

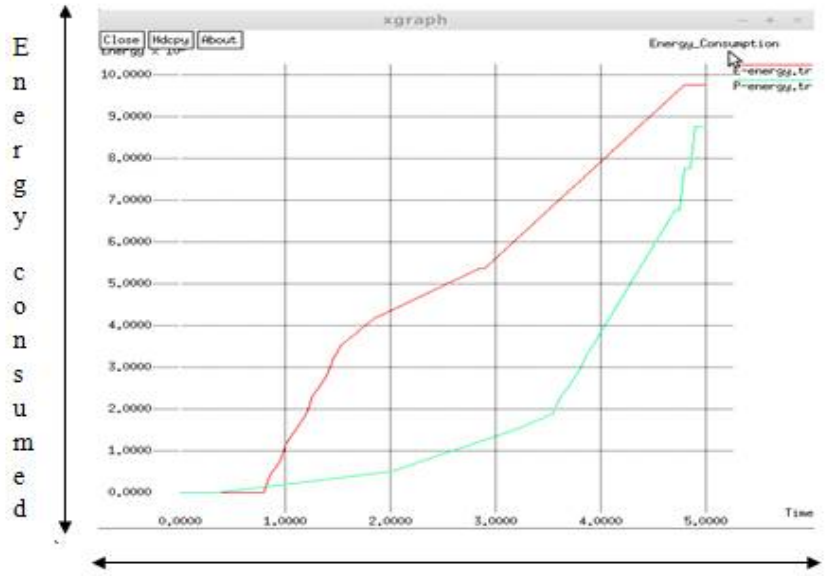

Fig.7.1 Energy Consumption

In case of any malicious or selfish node detected then the consumption of energy will be high. If the packets cooperates each other to reach the destination then it saves the energy and the low energy will be consumed in such cases.

PACKET DELAY

Traffic Rate	ET (Existing)	APT (Proposed)
1.0	59.226	59.031
2.0	69.227	69.032
3.0	79.227	79.032
4.0	89.227	89.033
5.0	99.227	99.034

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Table 7.2 Differences between the Packet Delay in Existing And Proposed Method

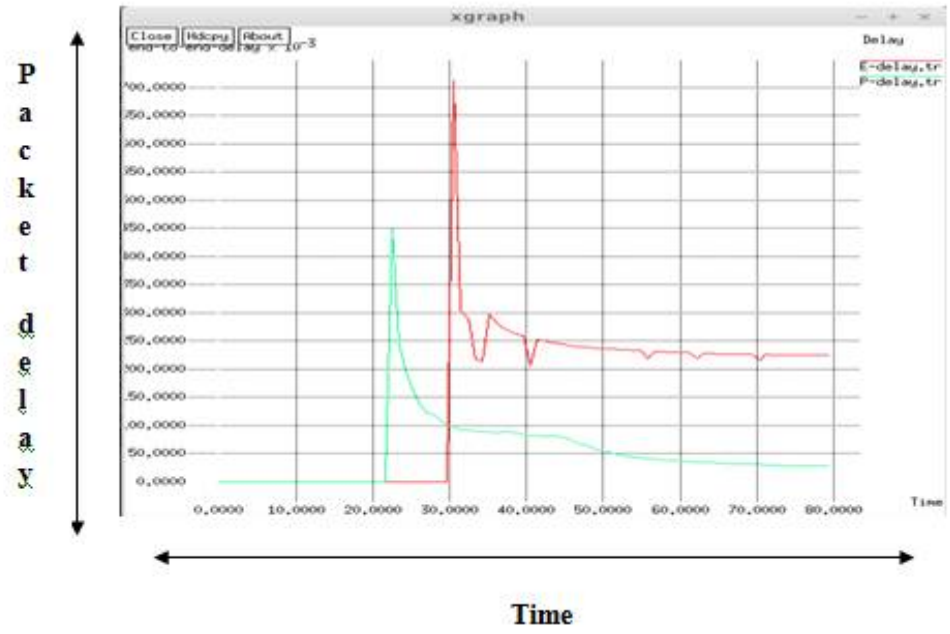

Fig.7.2Packet Delay

It shows the delay rate and its comparison of simulation result along with the existing work.

PACKET DELIVERY RATIO

Traffic Rate	ET (Existing)	APT (Proposed)
0.1	0.050	0.053
0.2	0.100	1.000
0.3	0.150	3.149
0.4	0.200	3.199
0.5	0.25	3.399

Table 7.3 Differences between the Packet Delivery Ratio in Existing And Proposed Method

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

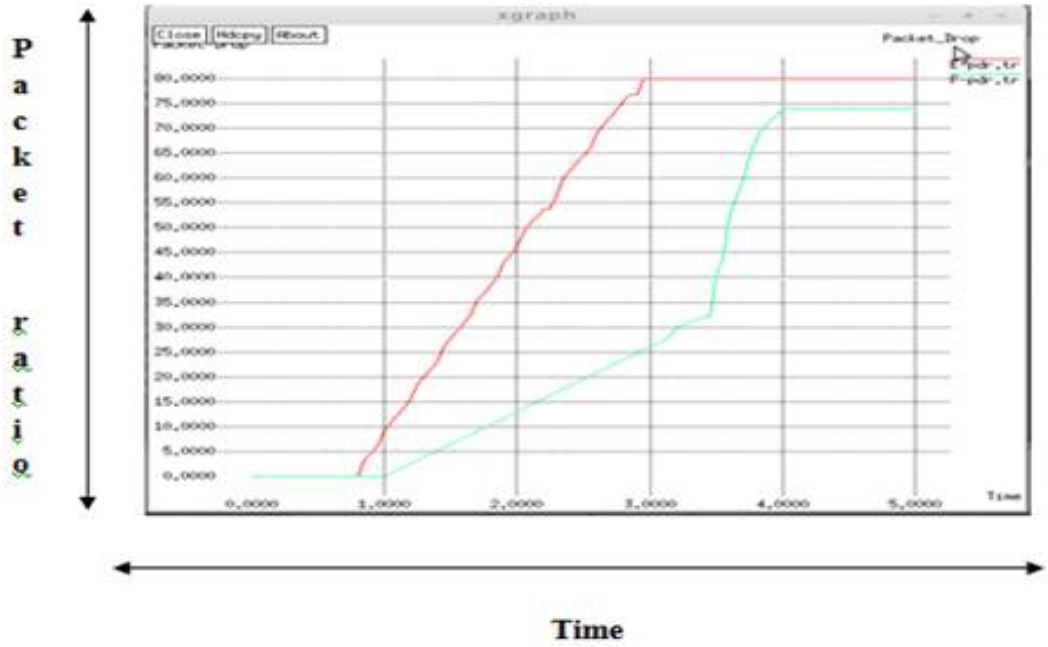

Fig.7.3Packet Delivery Ratio

It shows the comparison between the existing and the proposed strategy. It is seen that the proposed system gives the progressive ratio when comparing with the existing work.

THROUGHPUT

Traffic Rate	ET (Existing)	APT (Proposed)
0.1	1.250	1.350
0.2	2.300	4.330
0.3	2.480	4.865
0.4	3.200	5.122
0.5	4.750	5.877

Table 7.4 Differences between the Throughput in Existing And Proposed Method

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

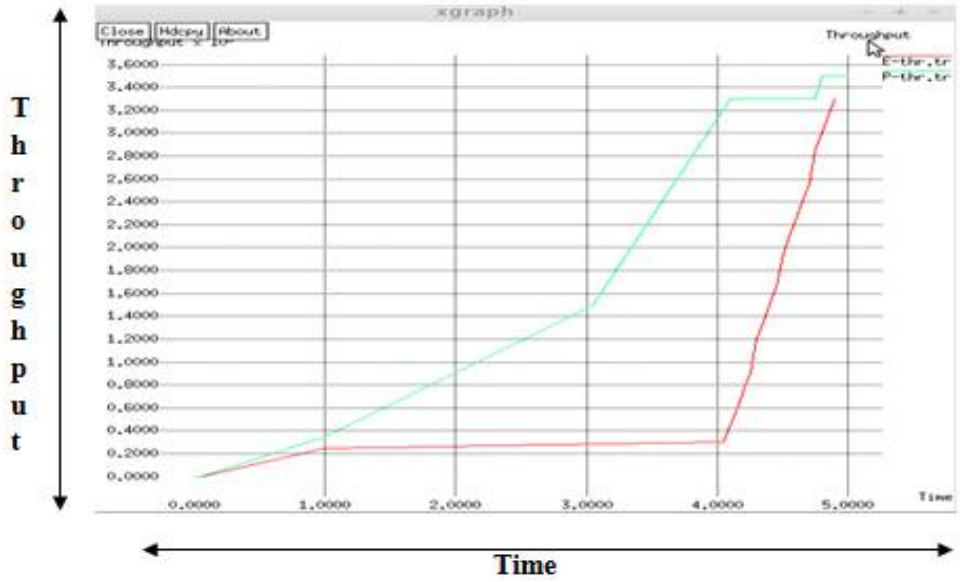

Fig.7.4 Throughput

It shows the performance evaluation of throughput that is compared between the existing and the proposed. The comparison is based on the traffic bit rate.

`

VIII. CONCLUSION AND FUTURE WORK

In wireless sensor network, the security issues are the major concern. In the security issues secure routing is one main concept to achieve security in WSN. In this paper it is also discussed the various existing methods to find the trusted node and secure routing. From all the work it is concluded that, this provides the high level of security, and secure routing with energy efficient and reduced overhead.A WSN's trust scheme is an important aspect of WSN security. In this paper, WSN node trust the particular node of packets, that has to be send and trust allocation problems using Airport based game theory.

Based on the interaction cooperation of the sensor nodes, consider the data retransmission after packets are lost and the trust incentive mechanism and build an Airport game model that is closer to the reality of WSNs. Moreover, the proposed Airport problem game theory is a problem that solves by sharing or dividing the cost or whatever so equally to the network (i.e players in terms of games) , it is mainly known as cost allocation. By drawing the conditions of reaching a steady state and analyze the factors that affect the convergence speed, and, finally, it is compared that this suitable game solution is applicable and it is also proved effectively and feasibly by several experiments.

The results of this work reveals the allocation rules of trust decision-making and trust evolution of WSNs.

The performance evaluation of metrics in this work can be concluded by divulging the solved networking parameters namely Energy consumption, Packet drop, Packet delay and Throughput. In accordance to the evaluation result Energy consumption, Packet drop, Packet delay show the accurate performance to the system. When comparing the Proposed with the Existing where it shows the differences of 2% satisfaction and meets its requirements.

Throughput in accordance to the evaluation result it has given an upright performance to the system. In this proposed result the energy consumption is low when compared to existing results, In case of both the packet delay and packet drop is also low when compared to the existing results.

In future, the scholars can look into scenarios utilizing the analytical model to find the trust requirementsThe trust value calculation on observing these parameters further improves the identification of various kind of attacks. As a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

future work trust model can be built to observe the proposed parameters and evaluate trust factors to ensure the detection of various attacks. This work is also related to trust based secure communication in wireless sensor networks**.**

Moreover it is also mainly focused on the routing by which the selfish node is detected and the particular selfish node is isolated in order to continue the process of communication from the source to the destination. In future, this work can be designed using cryptographic technology for security issues since WSN has lot of security issues so this cryptographic technique can help some of the issues so in future work such techniques can be used.

REFERENCES

1. A. Boukerche, X. Cheng, and J. Linus, "Energy-aware data-centric routing in microsensor networks", Proceedings ACM MSWiM, in conjunction with ACM MobiCom, San Diego, CA, Sept. 2003, pp. 42- 49.
2. A. Manjeshwar and D. P. Agrawal, "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks", in the Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.
3. A. Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks", in the Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, San Francisco CA, April 2001, pp. 2009-1015.
4. B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", Proceedings ACM MobiCom'00, Boston, MA, Aug. 2000, pp. 243-254.
5. B. Nath and D. Niculescu, "Routing on a curve", ACM SIGCOMM Computer Communication Review, vol. 33, no.1, Jan. 2003, pp. 155-160.
6. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", Proceedings ACM MobiCom'00, Boston, MA, Aug. 2000, pp. 56-67.
7. C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking", IEEE/ACM Transactions on Networking, vol. 11., no. 1, Feb. 2003, pp. 2- 16.
8. D. Braginsky and D. Estrin, "Rumor routing algorithm in sensor networks", Proceedings ACM WSNA, in conjunction with ACM MobiCom'02,Atlanta, GA, Sept. 2002, pp. 22-31.
9. G. Xing, C. Lu, R. Pless, and Q. Huang, "On greedy geographic routing algorithms in sensing-covered networks", Proceedings ACM MobiHoc'04, Tokyo, Japan, May 2004, pp. 31-42.
10. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks (Elsevier) Journal, Vol. 38, no. 4, Mar. 2002, pp. 393-422.
11. J. Luo, and J.- P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks", Proceedings IEEE INFOCOM'05, vol. 3, Miami, FL, Mar. 2005, pp. 1735-1746.
12. J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", Wireless Networks, vol. 8, no. 2/3, Mar.-May 2002, pp. 169- 185.
13. K. Akkaya and M. Younis, "An Energy-Aware QoS Routing Protocol for Wireless Sensor Networks," in the Proceedings of the IEEE Workshop on Mobile and Wireless Networks (MWN 2003), Providence, Rhode Island, May 2003
14. Lan Wang and Yang Xiao, "A Survey of Energy-Efficient Scheduling Mechanisms in Sensor Network".
15. L. Li and J. Y. Halpern, "Minimum-energy mobile wireless networks revisited", Proceedings IEEE ICC'01, Helsinki, Finland, June 2001, pp. 278-283.
16. Shio Kumar Singh , M P Singh , and D K Singh "Routing Protocols in Wireless Sensor Networks –A Survey" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010
17. M. Chu, H. Haussecker, and F. Zhao, "Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks", International Journal of High Performance Computing Applications, vol. 16, no. 3, Feb. 2002, pp. 293-313.
18. M. Zorzi and R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: Mutlihop performance", IEEE Transactions on mobile Computing, vol. 2, no. 4, Oct.-Dec. 2003, pp. 337-348.
19. N. Sadagopan, B. Krishnamachari, and A. Helmy, "The ACQUIRE mechanism for efficient querying in sensor networks", Proceedings SNPA'03, Anchorage, AK, May 2003, pp. 149-155.
20. OssamaYounis and Sonia Fahmy, "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-efficient Approach", September 2002. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010 82
21. OssamaYounis and Sonia Fahmy" Heed: A hybrid, Energy-efficient, Distributed Clustering Approach for Ad-hoc Networks", IEEE Transactions on Mobile Computing, vol. 3, no. 4, Oct.-Dec. 2004, pp. 366-369.
22. R.C. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling a three-tier architecture for sparse sensor networks ", Proceedings SN P A '03, Anchorage, AK, May 2003, pp. 30-41.
23. RenjianFeng, Xiaona Han, Qiang Liu, and Ning YuA Credible Bayesian-Based Trust Management Scheme for Wireless Sensor NetworksInternational Journal of Distributed Sensor Networks Volume 2015 (2015), Article ID 678926,
24. S.K. Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.
25. S. Lindsey and C.S. Raghavendra, "PEGASIS: Power-efficient Gathering in Sensor Information System", Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, MT, Mar. 2002, pp. 1125-1130.
26. S. Lindsey, C. S. Raghavendra, and K. M. Sivalingam, "Data gathering in sensor networks using the energy delay metric", Proceedings IPDPS'01, San Francisco, CA, Apr. 2001, pp. 2001-2008.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

27. S. Lindsey, C. S. Raghavendra, and K. M. Sivalingam, "Data gathering algorithms in sensor networks using energy metrics", IEEE Transactions on Parallel and Distributed Systems, vol. 13, no. 9, Sept. 2002, pp. 924-935.
28. T. He et al., "SPEED: A stateless protocol for real-time communication in sensor networks," in the Proceedings of International Conference on Distributed Computing Systems, Providence, RI, May 2003.
29. Vandana Jindal, A.K.Verma, SeemaBawa," How the two Adhoc networks can be different: MANET & WSNs " IJCST Vol. 2, Issue 4, Oct. - Dec. 2011 ISSN : 0976-8491 (Online) | ISSN : 2229-4333
30. V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks", IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, Aug. 1999, pp. 1333-1344.
31. W. Chang, G. Cao, and T. La Porta, "Dynamic proxy tree-based data dissemination schemes for wireless sensor networks", Proceedings IEEE MASS'04, Fort Lauderdale, FL, Oct. 2004, pp. 21-30.
32. W. Lou, "An Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks", Proceedings of IEEE MASS'05, Washington DC, Nov. 2005, pp. 1-8.
33. W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", Proceedings ACM MobiCom '99, Seattle, WA, Aug.1999, pp. 174-185.
34. W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks", in IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000, vol. 8, pp. 8020.
35. W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" in IEEE Tmnsactions on Wireless Communications (October 2002), vol. 1(4), pp. 660-670.
36. X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes", Proceedings IEEE VTC'05, Dallas, TX, Sept. 2005, pp. 2528-2532.
37. Y. X:u, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing", Proceedings ACM/IEEE MobiCom'01, Rome, Italy, July 2001, pp. 70-84.
38. Y. Yao and J. Gehrke, "The Cougar approach to in-network query processing in sensor networks", SGIMOD Record, vol. 31, no. 3, Sept. 2002, pp. 9-18.
39. Yuanjie Li, HongyunXu, Qiying Cao, Zichuan Li, and ShigenShen, Evolutionary Game-Based Trust Strategy Adjustment among Nodes in Wireless Sensor Networks Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, Article ID 818903, pages http://dx.doi.org/10.1155/2015/818903
40. Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks", Technical Report UCLA/CSD-TR-01-0023, UCLA Computer Science Department, May 2001.
41. ZhiRen, ShuangPeng, Hongjiang Lei, Jibi Li proposed Game Theory-Based Routing Algorithms for Wireless Multi-hop Networks, Proceedings of the 2012 2nd International Conference on Computer and Information Application (ICCIA 2012)