IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

A Trust Election Based Mechanism for Finding Selfish Node and Preventing Them from Attack

Priya Mishra[1*], Ompal Singh[2], Abhishek Bhatt[3]

[1,2,3]Dept. of Electronics & Communication, Technocrats Institute of Technology, Bhopal, India

Corresponding Author: priya.mishraews195@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i2.223229 | Available online at: www.ijcseonline.org

Accepted: 15/Feb/2019, Published: 28/Feb/2019

Abstract— Wireless sensor network is an important communication resource in wireless area. It enable to recognize many resources and file data such as temperature, humidity and many other dynamic functional data which needed observation. In many remote areas where the different terminology adaption is difficult while dealing with opposite situations wireless sensor network help in establish a proper communication between them. A proper network and communication also get disadvantage of intruder and anomaly within the network. WSN deals with attack resistance and finding such node which participate in such activity. Many algorithm used for finding such selfish attack nodes and preventing data from them. In this paper the proposed algorithm shown is proposed for the selfish node detection and prevention. The approach is performed using NS-2 simulation tool with dynamic node number selection model. The observe outcome while running the script observe high performance over existing scenario.

Keywords—Wireless Sensor Networks (WSN), MANET (Mobile AD-Hoc Networks), Selfish node, network failure, data packet transmission**.**

I. INTRODUCTION

Wireless Sensor Networks can be defined as the collection of the sensor nodes that collect the information or a data from this planet and then use it in the communication process through the wireless handsets. Generally, the sensor nodes used to work with the batteries and are frequently conveyed to not effectively available or unfriendly condition. MANET is a widely used network with a lot of users. In this type of network users need more security and surety against their data, which will not get fail in between the initial and the final stage. Because in some of the cases our confidential information which is travelling from a source to the destination without the presence of the security may lead to get an access to the third-party (unauthorized user) that will cause abusing of information [1].

There is one major issue which arises in the Wireless Sensor Networks is that it can easily get attacked by the Denial of A Service attacks (DoS) which causes a huge loss in the information and will have more energy expenses. Therefore, it is very important to design a network that will overcome the problem of the security.

Wireless sensor network(WSN) is a group of sensor nodes which gets uploaded in a practical life. These nodes may easily get affected by various intruders which are working hard to hack the unauthorized information.

The hubs called selfish hubs or nodes, expect to pick up the best advantages from the systems while endeavoring to save their own assets. The asset incorporates equipment, battery life or data transfer capacity. Selfish hubs just endeavor to speak with the hubs it needs to send information parcels to. They may decline to collaborate when it gets steering bundles or information parcels that they have no enthusiasm for. Consequently, they either drop information bundles or decline to retransmit steering parcels that they have no enthusiasm for.

In this paper, Tri Trust Evaluation DIRAA Model approach based on three level of trust computation over a node is used to finding a proper node values and their selfish node probability to keep or discard from the network.

II. RELATED WORK

SonaTaheri and Musa Mammadov are discussed Learning the Naive Bayes classifier with optimization models has proposed a concentrated blame ID framework for a WSN in light of the Naïve Bayes structure.[5] This methodology explored start to finish divide deferral to analyze the framework status. The impediment of this methodology was that it didn't work in a dynamic circumstance where compose topology a great part of the time changes on account of deficient centers. It required a broad time span to dissect the sensor hubs of the passed on sensor center points in significant scale WSNs and it also made a high volume of development through the focal blame examination center point. Consequently, this methodology isn't sensible for expansive scale WSNs.

Peng Jiang discussed A New Method for Node Fault Detection in Wireless Sensor Networks proposed a scattered figuring, named FDWSN for distinguishing and detaching broken sensor hubs from a WSN [6]. Defective sensor hubs in FDWSN were perceived in nearby examinations between the neighbor hubs. Each individual sensor settled on without anyone else decisions in perspective of the adjacent examination comes to fruition. This methodology reused flawed sensor hubs as correspondence hubs for information directing, anyway they are rationally disengaged from the system. This methodology endured transient blames through time reiteration amid the data trade process. The central detriment of this conveyed methodology was that each sensor center assembled data from their neighbor hubs on different occasions. In like manner this methodology expended more vitality contrasted and other appropriated blame discovery approaches. In addition this methodology did not consider transmission accuses that happen amid the issues determination process.

Abolfazl Akbari Nedal Beikmahdavi and Ali Khosrozadeh, Omid Panah are discussed A Survey Cluster-Based and Cellular Approach to Fault Detection and Recovery in Wireless Sensor Networks proposed a bound blame discovery approach for WSNs where each sensor hub thought about its own specific identified data and the center of its neighbor hubs data in order to break down its own prosperity status [7]. The impediment of this methodology is that, if all neighbors of the indicative sensor hubs are broken by then working symptomatic sensor hubs can recognize it as having a blame when a blame may not be accessible. Subsequently, the blame identification execution of this methodology is incredibly poor.

Meenakshi Panda and Pabitra Mohan Khilar are discussed Distributed Soft Fault Detection algorithm in wireless sensor networks utilizing Statistical Test proposed A three-sigma modify test based Distributed Soft Fault Detection (DSFD) approach was displayed [8]. In DSFD each sensor hub shared their own specific distinguished data to neighbor hubs with a particular ultimate objective to perceive plausible deficiencies of its own and neighbor hubs using the three-sigma change test. By then, plausible blame status was shared to the neighbor hubs. For blame determination each sensor hub thought about its own specific distinguished data and its neighbor hub recognized data and blame decisions were made dependent on an edge esteem. This methodology distinguished damaged hubs inside the framework, yet it didn't perceive the distinct gear and programming state of the conveyed sensor hubs. Thusly this methodology perceived various non-flawed hubs as deficient hubs amid the broken discovering stage and lessened the execution of the framework. In like manner, it was not ready to endure any correspondence interface disillusionment issues amid the data trade process.

Amol Shende1and Prof. Vikrant Chole2 are discussed A Review on Improving Packet Analysis in wireless sensor network utilizing Bit Rate Classifier proposed about PCMA [9]. Past written works were shown as of late to fixate on the most proficient method to perceive the childish hubs in MANET with base on the discovery techniques to talk about. They proposed another part called Packet Conservation Monitoring Algorithm (PCMA) to perceive the childish hubs in MANET. A guard dog strategy was shown. This framework can perceive those hubs that have mischievous activities in MANET. In addition the other instrument called way rate furthermore was presented. This instrument can keep that the transmission ways depend on those hubs that have mischievous activities. Use an OCEAN layer to empower hubs to enable hubs to settle on astute steering and sending choices. By the OCEAN systems they can recognize and direct misleading coordinating behavior in MANET.

Charles E. Perkins discussed Ad-hoc On-Demand Distance Vector Routing [10]. center around four kind of the narrow minded practices to propose the location techniques.
Vigna et al have proposed a way to deal with identify interruptions in AODV that works by stateful mark based investigation of the watched traffic [11] .

Pirzada and McDonald have portrayed a model of building trust connection between hubs in a specially appointed system [12]. The hubs latently screen the parcels got and sent by different hubs and process the trust esteems for their neighbors. The trust esteems are utilized for registering the dependability of connections. For directing joins with high trust esteems are picked in order to maintain a strategic distance from the noxious and narrow minded hubs.

Conti et al have proposed a plan in which a hub misuses its neighborhood information to assess the unwavering quality of a way [13] . In contrast to the customary technique for denying narrow minded clients, it gives a corrupted support of these hubs by particular moderate parcel sending.

Santhanam et al have exhibited a system to pass judgment on a hub's conduct dependent on watched traffic reports submitted to nearby sink operators, scattered all through the system [14]. The sink hubs apply a lot of sending tenets to detach a childish hub dependent on the occasions it is gotten in egotistical acts. The plan is free of the directing convention or system design and is appropriate for multi-channel remote work organize.

Thus the approach given in past are limited to some area such as working with low speed data packet processing. It also takes monitoring of low bandwidth and in data monitoring takes high bandwidth consumption.

III. PROBLEM FORMULATION

As per discussion of previous solution provided, there are limitations in architecture provided. The algorithm observed having the following limitation which can further resolve.

1. A Proper communication guidance between the intermediate nodes. Also it is related with the current data usage and sharing.
2. A proper data dissemination and utilization of framework. Finding selfish faulty node policy among the available nodes.
3. Finding a virtual network and optimizing the data usage over it if the network faulty nodes are found in between. Thus a proper data transmission in such environment is required.
4. A multiple way point cooperation and trust generation co-efficient which can produce the efficient outcome on selfish node detection is not introduced.

Thus the given issues can further worked to overcome and finding the solution on it.

IV. PROPOSED METHODOLOGY

In order to overcome the given limitation of node cooperation and generating the value measure. The recommendation based trust model with a defense scheme to filter out attacks related to dishonest recommendations like castigating, vote stuffing, and plot for versatile specially appointed systems. The suggesting hub is picked dependent on three elements to check its genuineness: number of connections with the assessed hub, solidarity of view with the assessing hub for taking care of the issue of the shortage of learning, closeness to the assessing hub. Suggestions are aggregated over some undefined time frame to guarantee the consistency of proposals given by are praising hub with respect to the assessed hub. Flow Architecture: The following is the setup flow architecture which is following at the selfish node detection level Network module.

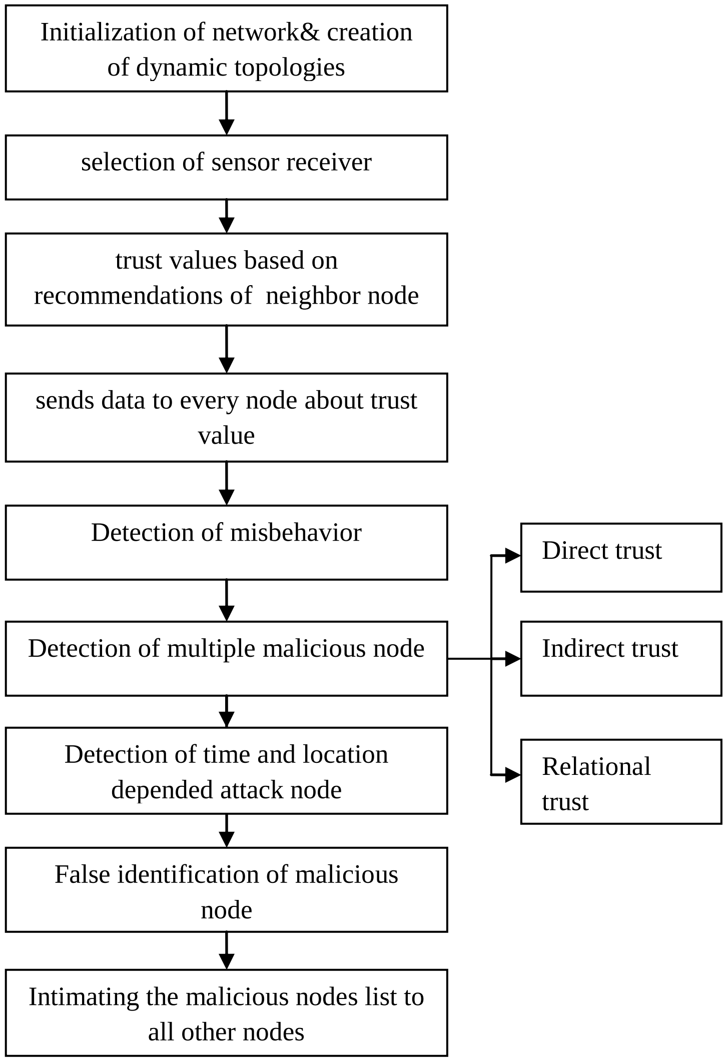
Initialization of network& creation of dynamic topologies
selection of sensor receiver
trust values based on recommendations of neighbor node
sends data to every node about trust value
Detection of misbehavior
Detection of multiple malicious node
Direct trust
Indirect trust
Relational trust
Detection of time and location depended attack node
False identification of malicious node
Intimating the malicious nodes list to all other nodes

Figure 1: Flow of overall detection process.

- Routing Protocol module.
- Node Module.
- OSI layer module.
- Attacker module.
- Trust computation component

The figure 1 above shows the overall proposed flow architecture processed .

The Complete algorithm is initialized and stepped as given pseudo code with the three level of trust computation and finally finding the minimal trust summation computation. Following are the steps which used in the proposed algorithm.

1. Initializing all the nodes with their initial configuration and node positioning with the axis value.

2. Providing input node numbers, source node and destination node. This is the communication node on which transmission of data is going to get performed over the network.

3. Starting communication over the network after assigning an initial node trust value and energy value.

4. Initializing the procedure by computing the trust values upon each iteration till it reach to the destination node. Three level of trust computation is performing to find the Minimum utilization node through which data can be transmitted by maximizing its life time.

5. Direct trust, indirect trust and relational trust computation is performed through the node selection for enroute.

6. Direct trust computation is performed :

$Dn = \{f - (d + m)\}/f$ ....(1)

f is number of packet forwarded;
d is packet number dropped,
m is number of packet misrouted.

7. Indirect Trust computation is performed:

$$ID = (Access\ control + Edge\ Connected + Reachability\ to\ destination) / Time\ estimation\ for\ successful\ transmission;$$

$IDn = Ac + Ec + Rd/Te$ ....(2)

8. Relational trust computation:

$Rt = Successful\ interaction + (Tcn + Ecn + Mobility\ Estimation)$ ....(3)

Tcn is trust consumption estimation;
Ecn is Energy consumption estimation;

9. Finding minimum energy consumption probability node using summation of three trust computed.

Packet transmission node

$Pn = \sum Min\ (Dt + IDt + Rt)$; ....(4)

10. Performing data transmission over safe node and performing the trace generation of complete scenario.

11. Computing result obtained and plotting them using the x graph functionality of available platform.

V. EXPERIMENTAL SETUP

To implement proposed technique, NS2 simulator is used which provides an enhanced functionality to develop research projects for communication network. In that way it provides a framework to develop such projects.

Network simulator is used to analyze the traditional communication node failure detection and modified trust election based mechanism for communication in WSN. The existing is run on this simulator and with same environment this simulator will again run for Modified optimized election to show the comparison of performance on parameters: end-to-end Delay, Packet Delivery Ratio (PDR), Throughput and energy.

The Modified Technique is simulated with following scenarios:

Table 1: Simulation Scenarios

No. of Nodes	46
No. of Source	10
Area	1000X1000
Mobility model	Random waypoint
Bandwidth	2mbps
Speed	0,1,5,10,15,20m/s
Pause time	10 sec
Buffer Size	100
Transmission range	2100m
Sensing range	2100m
Packet size	1012bytes
Traffic source	Constant Bit Rate (CBR)
MAC protocols	IEEE 802.11

Table. 1 above, shows the parameter values which is taken for the simulation setup over NS-2 networking platform for data packet transmission.

VI.RESULT ANALYSIS & DISCUSSION

A comparison analysis for the results for existing and proposed technique is shown in this section.

Evaluation Parameter : Transfaulty node , Throughput , packet loss, PDR (Packet Delivery Ratio) , packet delay , End-to-End Delay are used to calculate performance of technique.

Transfaulty node:- which cause disturbance in communication network. That means neighbour node accept data packet but cannot forward in next node.

Throughput:- numbers of successfully data which comes on destination. Or It is the measure of whole performance of the network according to the time .

Packet loss:- Packet loss is the failure of one or more transmitted packet to arrive at their destination.

PDR (Packet Delivery Ratio):- It is the ratio of, no. of packet accurately delivered to the destination. Receive packet/ total time

Packet Delay:- It is measure of time taken to getting response to deliver packet from source to destination.

End-to-end delay:- End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. ∑ (arrive time – send time) / ∑ Number of connections

A graphical analysis for the proposed technique is shown in graph, which shows a graphical comparison over the technique

Table 2: Packet Loss Vs Transfaulty node.

Packet Loss Vs Transfaulty node			
TF	No Rescue	Existing	Proposed
0%	0.2	0.2	0.18
10%	0.31	0.19	0.18
20%	0.39	0.2	0.18
30%	0.43	0.19	0.17
40%	0.48	0.2	0.16
50%	0.6	0.2	0.15

In the above table 2 the comparison in between the previous algorithm and the proposed algorithm on the basis of packet loss and transfaulty nodes has been shown.

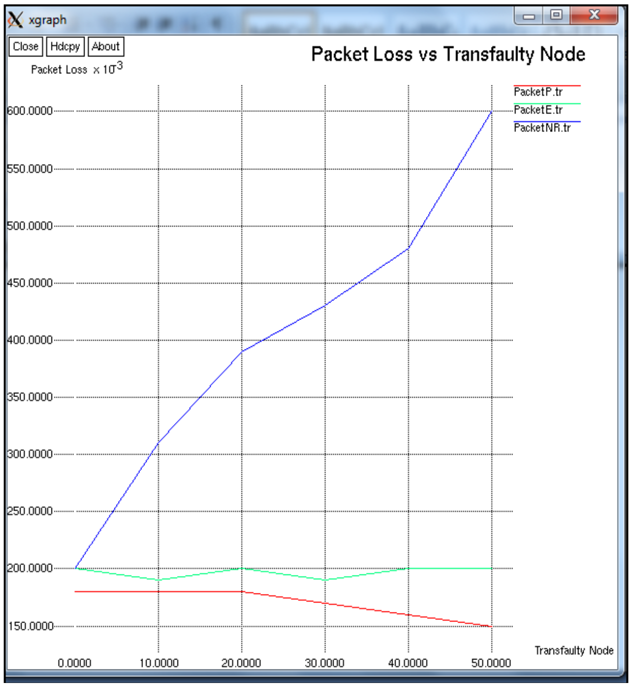

Figure 2: Packet Loss Vs Transfaulty node

Transmission Time:

Table 3: Transfaulty node VS Time.

Transfaulty node VS Time			
Time	**No Rescue**	**Existing**	**Proposed**
0	**0.30**	**0.30**	**0.28**
50	**0.39**	**0.29**	**0.29**
100	**0.6**	**0.31**	**0.28**
150	**0.9**	**0.32**	**0.28**
200	**0.9**	**0.31**	**0.29**
250	**0.91**	**0.35**	**0.3**

In the above figure. 3 we have shown the graphical representation of the obtained values on the basis of transmission time which is clear that time is decreases as compared to the previous algorithm.

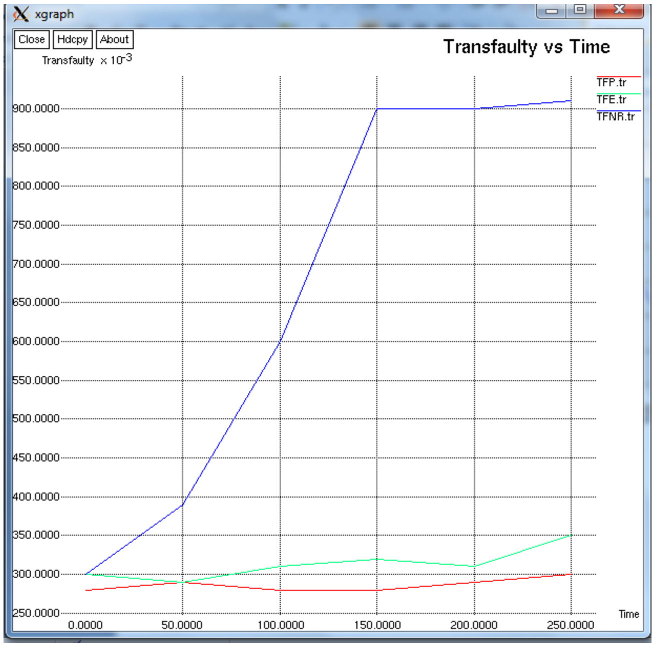

Figure 3: Transfaulty node vs time

Throughput:

Table 4: Throughput VS Transfaulty Node

Throughput VS Transfaulty Node			
TF	**No Rescue**	**Existing**	**Proposed**
0%	**0.8**	**0.8**	**0.84**

10%	**0.69**	**0.79**	**0.83**
20%	**0.63**	**0.79**	**0.81**
30%	**0.55**	**0.78**	**0.8**
40%	**0.51**	**0.79**	**0.79**
50%	**0.51**	**0.76**	**0.78**

In the above table .4 the comparison in between the previous and the proposed algorithm is done on the basis on throughput.

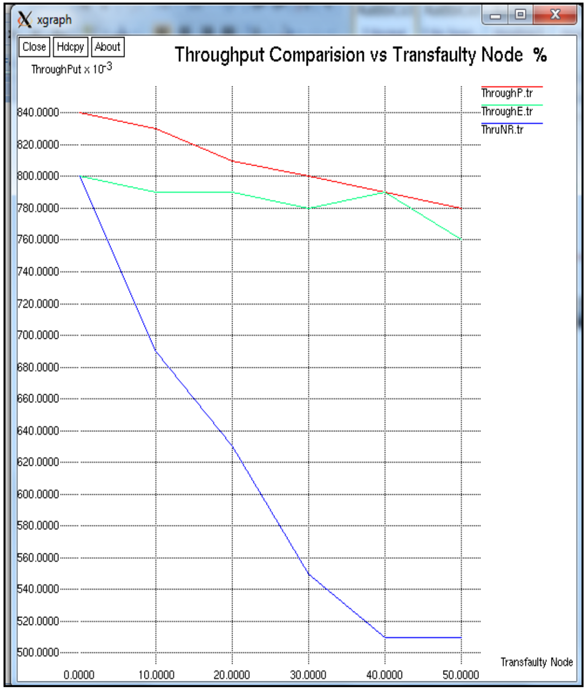

Figure 4: Throughput vs transfaulty node.

The above figure 4 shows the throughput changes in proposed work, it increases in this work.

Table 5: Packet Delay Vs Time.

Packet Delay Vs Time		
Time	**Existing**	**Proposed**
0	**0.96**	**0.95**
50	**0.94**	**0.93**
100	**0.92**	**0.90**
150	**0.90**	**0.88**
200	**0.89**	**0.85**
250	**0.88**	**0.86**

In the above table 5 the comparison among the packet delay vs time has been shown.

The above figure. 5 shows the Packet delay time changes in proposed work, it decreases in the proposed work as compare to exiting work.

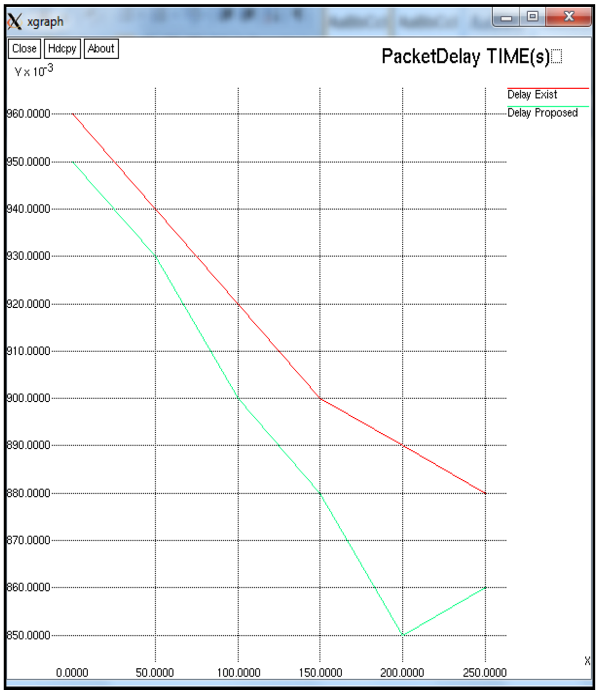

Figure 5: Packet delay time.

A description over the implementation scenario to implement proposed technique and evaluation of the results of the technique is presented. On the evaluation presented in result analysis section, evaluation over all the parameter shows that, proposed technique provides better results as compare to the existing technique.

VII.CONCLUSION & FUTURE SCOPE

Selfish node over the wireless sensor network is important point to monitor. Selfish node over the wireless sensor network is important point to monitor. The activity of such node makes data leak and hence damaging of information obtained from different resources. WSN acquire many important information which help in taking further decisions. In this paper the approach which is trust based selfish node detection and prevention is proposed. The algorithm use trust management and election mechanism. As per the results which we have got after applying the propose algorithm Trust based selfish node detection and prevention method on several aspects which can be described as: First we had calculate packet loss with respect to transfaulty node (0%-50%) and that will increase for the proposed algorithm as compared to the previous algorithm. Second we had done calculation of transfaulty node with respect to time (from 0-250msec) which in proposed algorithm case tends to decrease constantly. Third we will calculate throughput with respect to transfaulty node (from 0%-50%) and throughput will constantly increase. Fourth we will calculate packet delay with respect to time (0-250 msec) and packet delay is decrease in proposed technique as compare to exiting approach.

Wireless and network node plays an important role while computing the communication usage. Anomaly nodes and saving energy is always an action which is needed in any of the routing technique. Thus the proposed TriTrust based technique is proposed. Still there are following future work which can be considered as upgradation of proposed work scenario.

1. Working with energy saving module and sharing of resources using some centralized communication main node.
2. Implementation of catching and hence pre-determination of pre-visited nodes. Which can reduce computation time while working with communication cost.
3. An implementation of proposed work can be extended with NS3 implementation.
4. Finding more parameters for the computation and other techniques through which more efficient comparison can be performed.

REFERENCES

[1] Pushpendu Kar, Student Member, IEEE and Sudip Misra, Senior Member, IEEE, Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes, 1932-4537 (c) 2015 IEEE.

[2] Abdul Razaque, M. Abdulghafour, Meer Jaro Khan, Detection of Selfish Attack over Wireless Body Area Networks, 2017 IEEE Conference on Open Systems (ICOS), November 13-14, 2017, Miri, Sarawak, Malaysia.

[3] JaydipSen, and Kaustav Goswami2, an Algorithm for Detection of Selfish Nodes in Wireless Mesh Networks, Oct. 28-30, 2009.

[4] Naveen Kumar Gupta, **Ashish Kumar Sharma, Abhishek Gupta, Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS), Volume-1 Issue-2, September 2012.

[5] SonaTaheri, Musa Mammadov , Learning The Naive Bayes Classifier With Optimization Models, Vol. 23, No. 4, 787–795 DOI: 10.2478/amcs-2013-0059.

[6] Peng Jiang, A New Method for Node Fault Detection in Wireless Sensor Networks, 24 February 2009.

[7] AbolfazlAkbari, NedaBeikmahdavi, Ali khosrozadeh, OmidPanah, A Survey Cluster-Based and Cellular Approach to Fault Detection and Recovery in Wireless Sensor Networks, Journal 8 (1): 76-85, 2010.

[8] Meenakshi Panda, Pabitra Mohan Khilar, Distributed Soft Fault Detection Algorithm in Wireless Sensor Networks using Statistical Test, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[9] Amol Shende1, Prof. Vikrant Chole2, A Review on Improving Packet Analysis in Wireless Sensor Network using Bit Rate Classifier, Vol.5 Issue.6, June- 2016, pg. 102-107.

[10] Charles E. Perkins, Ad-hoc On-Demand Distance Vector Routing.

[11] G. Vigna, S. Gwalani, K. Srinivasan, E.M. Belding-Royer, and R.A. Kemmerer, “An intrusion detection tool for AODV-based ad hoc wireless networks,” in Proc of Annual Comp. Sec. Appl. Conf (ACSAC) 2004, pp. 16-27.

[12] A. Pirzada and C. McDonald, “Establishing trust in pure ad hoc networks,” in Proceedings of the 27th Australian Conference on Computer Science, 2004, pp. 181-199.

[13] M. Conti, E. Gregori, and G. Maselli, “Reliable and efficient forwarding in MANETs,” Ad Hoc Networks Journal, Vol 4, No 3, 2006, pp. 398-415.

[14] L. Santhanam et al, “Distributed self-policing architecture for fostering node cooperation in wireless mesh networks,” in Proc. of PWC 2006, Vol 4217, pp. 147-158.

[15] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, RFC 3775, June 2004

[16] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, Network Mobility (NEMO) Basic Support Protocol, RFC 3963, January 2005

[17] T. Ernst, H-Y. Lach, Network Mobility Support Terminology, draftietf-nemo-terminology-04.txt, October, 2005

[18] A.Vani ,Detection and Elimination of Wormhole Attacks in a MANET ,Int. J. Sci. Res. in Computer Science and Engineering Vol-5(5), Oct 2017,

[19] Dipali Koshtiand Supriya Kamoji ,Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks IJSCE Volume-1, Issue-4, September 2011

[20] Neenavath Veeraiah, Dr.B.T.Krishna Selfish ,Node Detection IDSM Based Approach Using Individual Master Cluster Node in Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018) IEEE