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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

Performance Analysis of Implementation of Trust Aware Routing Framework (TARF) for Large Scale WSNs

Ms. Dipali G. Dikondwar[1], Prof. R. K. Krishna[2]

M Tech Student, Department of Computer Technology, R C E R T, Chandrapur (Maharashtra), India[1]

Assistant Professor, Department of Electronics Engineering, R C E R T, Chandrapur (Maharashtra), India[2]

ABSTRACT: Wireless Sensor Networks are gaining popularity due to the fact that they offer low-cost solutions for a variety of application areas, but efficient defence against security attacks is a challenging task in the wireless sensor network environment. However, these networks are highly susceptible to attacks, due to both the open and distributed nature of the network, as well as the limited resources of the nodes, which dictate the implementation of sophisticated security frameworks. In this paper we are studying the performance analysis of the previously simulated and implemented trust aware routing framework in various wireless node scenarios.

Keywords: WSN, trust-aware routing, energy efficient routing, secure routing, sensor energy, throughput, jitter, control overhead, simulation, dropping ratio, delay.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are invading our everyday life with their proliferating applications which cover environmental observation, homeland security, building and factory monitoring and personal healthcare [2]. The small dimensions of sensor nodes combined with their low cost, further contribute towards wider penetration leading to exponentially increase of the number of deployed sensor nodes in the near future [2]. Due to recent technological advances, the manufacturing of small and low-cost sensors has become technically and economically feasible. These sensors measure ambient conditions in the environment surrounding them and then transform these measurements into signals that can be processed to reveal some characteristics about phenomena located in the area around these sensors. A large number of these sensors can be networked in many applications that require unattended operations, hence producing a wireless sensor network (WSN). Even from their earliest deployments, sensor networks have been attacked by adversaries interested in intercepting the data being sent or reducing the ability of the network to carry out its tasks. As the applications of WSNs become more complex and widespread, the ability to protect such systems has become increasingly important. Although military applications seem to have the strictest security requirements, issues like data confidentiality, data integrity and network availability are also important to any WSN application [2]. The implementation of trust aware routing framework aims to secure routing solutions in wireless sensor networks. And in this paper we are studying the performance of the framework in various nodes arrangements.

Rest of the paper is organized as assumptions in II, implementation in III, performance evaluation in IV, graphical analysis in V, and conclusion in VI.

II. ASSUMPTIONS

In a data collection task, a sensor node sends its sampled data to a remote base station with the aid of other intermediate nodes. There could be more than one base stations, our routing approach is not affected by the number of base stations. Still for simplification purpose we are assuming here only one base station. We assume a data packet has at least the following fields: the sender id, the sender sequence number, the next-hop node id (the receiver in this one hop transmission), the source id (the node that initiates the data), and the source's sequence number [3].

III. IMPLEMENTATION

Data transmission accounts for a major Portion of the energy consumption. We evaluate energy efficiency by the average energy cost to successfully deliver a unit-sized data packet from a source node to the base station, be given enough attention when considering energy cost since each re-transmission causes a noticeable increase in energy consumption. If every node in a WSN consumes approximately the same energy to transmit a unit-sized data packet, we can use another metric hop-per-delivery to evaluate energy efficiency [3].

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

A. SIMULATION IN WSN

Implementation of WSNs can be done using various tools. Network simulators like OPNET, NetSim and NS2 can be used to simulate a wireless sensor network. Here we are using NS-2 as a network simulator with TCLscripting and C++ programming language. NS-2 as a non-specific network simulator can support a considerable range of protocols in all layers. For example, the ad-hoc and WSN specific protocols are provided by NS-2. Secondly, the open source model saves the cost of simulation, and online documents allow the users easily to modify and improve the codes [4].

B. METHODOLOGY

In energy module, each node relies on its neighbourhood table to select an optimal route, considering energy consumption and reliability. The neighbour energy cost is calculated by

Nb_energy_cost= (e_unit/p_succ)+ e_b

where e_unit= e_b/distance

p_succ= probability of the request message being acknowledged

According to neighbourhood table of energy values forwarding decision is taken [5]. In this simulation, we are considering a network of 100 wireless sensor nodes and one base station at the centre of the network.

IV. PERFORMANCE EVALUATION

In performance evaluation we are considering two different node arrangement networks and comparing the results of the two scenarios. Out of the two networks, we have timely results of one of the networks.

The following table shows the result values of the 10*10 flat grid Network as the simulation time progresses in three cases i. e. a normal network, a network with attackers and a network without attacker nodes. The various simulation parameters are considered to evaluate the results with simulation.

TABLE 1
THE 10*10 FLAT GRID NETWORK RESULTS WITH SIMULATION TIME

Simulation Parameters ↓	**Simulation time line**					
		50	75	100	125	150
Average Energy (Joules)	Normal	0.0175245	0.016168	0.014513	0.0155733	0.0158747
	With Attack	0.0105495	0.0240438	0.0385778	0.0551716	0.0710519
	Without Attack	0.0122013	0.0259002	0.0419279	0.0585131	0.0759265
Jitter (Seconds)	Normal	0.0899837	0.0786427	0.129334	0.109077	0.179691
	With Attack	0.0994311	0.0744839	0.0791866	0.0795387	0.0755526
	Without Attack	0.0555158	0.0531352	0.0527767	0.0526193	0.0525292
Throughput (bits/sec)	Normal	45423	51436.6	30959	37267.3	22478.8
	With Attack	40570.1	54607	51559.6	51011.3	54107.2
	Without Attack	72278.5	76571.8	77102.3	77588	77778.4
Dropping Ratio (%)	Normal	44.8	37.6	62.4	54.6	72.6
	With Attack	50.6667	33.375	37.1538	37.8679	34.0287
	Without Attack	12	6.75	5.92308	5.333333	5.08696
Control Overhead	Normal	2180	2693	3184	3713	4217
	With Attack	1471	2502	3538	4555	5592
	Without Attack	1492	2530	3553	4567	5573
Normalized Routing Overhead (%)	Normal	7.89855	8.63141	16.9362	16.3568	30.781
	With Attack	9.93919	4.69418	4.33048	4.0706	3.68379
	Without Attack	5.65152	3.39142	2.90515	2.68016	2.55291
Delay (Seconds)	Normal	0.0269452	0.0252847	0.0252146	0.0243216	0.0236592
	With Attack	0.0261243	0.025851	0.0251635	0.0259386	0.0265128
	Without Attack	0.0287059	0.0278658	0.0286226	0.0294983	0.0303392
Packet Delivery Ratio (%)	Normal	55.2	62.4	37.6	45.4	27.4
	With Attack	49.3333	66.625	62.8462	62.1321	65.9713
	Without Attack	88	93.25	94.0769	94.6667	94.913

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

In the following table, the overall network performance is calculated for the 10*10 network arrangement.

TABLE II

THE NETWORK PERFORMANCE ANALYSIS FOR 10*10 FLAT NETWORK WITH SIMULATION TIME

	NORMAL NETWORK	WITH ATTACK	WITHOUT ATTACK
No of pkts sent	3103	3101	3104
No of pkts recv	3033	2239	3072
Pkt delivery ratio	97.7441	72.2025	98.9691
Control Overhead	7625	7498	7675
Normalized Routing overheads	2.51401	3.34882	2.49837
Delay	0.0321964	0.0265813	0.0331646
Throughput	80252.3	59214.2	81235.6
Jitter	0.0505019	0.0684645	0.0498961
No of Pkts Dropped	70	862	32
Dropping Ratio	2.25588	27.7975	1.03093
Total Energy Consumption	13.9998	10.9135	14.6489
Average Energy Consumption	0.139998	0.109135	0.146489
Overall Residual Energy	9986	9989.09	9985.35
Average Residual Energy	99.86	99.8909	99.8535

The table 3 shows the performance analysis of the random arrangement of the 100 node network with and without attack.

TABLE III
OVERALL NETWORK PERFORMANCE ANALYSIS FOR RANDOM 100 NODE NETWORK WITH SIMULATION TIME

	NORMAL NETWORK	WITH ATTACK	WITHOUT ATTACK
No of pkts sent	3100	2301	2300
No of pkts recv	1660	1518	2183
Pkt delivery ratio	53.8065	65.9713	94.913
Control overhead	7409	5592	5573
Normalized routing overheads	4.44185	3.68379	2.55291
Delay	0.0268036	0.0265128	0.0303392
Throughput	44104.9	54107.2	77778.4
Jitter	0.0927512	0.0755526	0.0525292
No of Pkts Dropped	1432	783	117
Dropping Ratio	46.1935	34.0287	5.08696
Total Energy Consumption	8.36858	7.10519	7.59265
Average Energy Consumption	0.0836858	0.0710519	0.0759265
Overall Residual Energy	9991.63	9992.89	9992.41
Average Residual Energy	99.9163	99.9289	99.9241

V GRAPHICAL ANALYSIS

In the performance evaluation process graph play an important role. While studying the two different types of node arrangement networks we got some performance graphs. Out of those we are showing here the graphs for the 10*10 flat grid network. While doing the graphical analysis we considered the three cases a normal network, a TARF enabled network with attack and a TARF enabled network without attack.

The following graphs consider various parameters like average energy, throughput, delay, jitter, dropping ratio, normalized routing overheads, control overheads, packet delivery ratio etc.

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

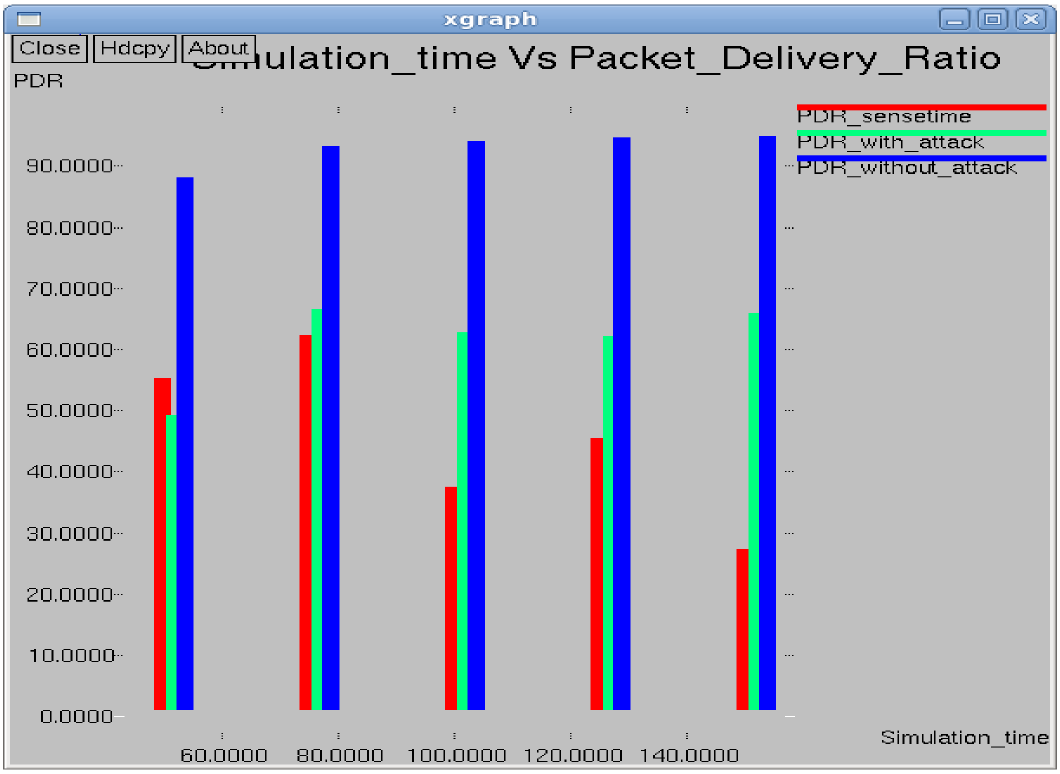

Fig. 1. Simulation time Vs Packet Delivery Ratio

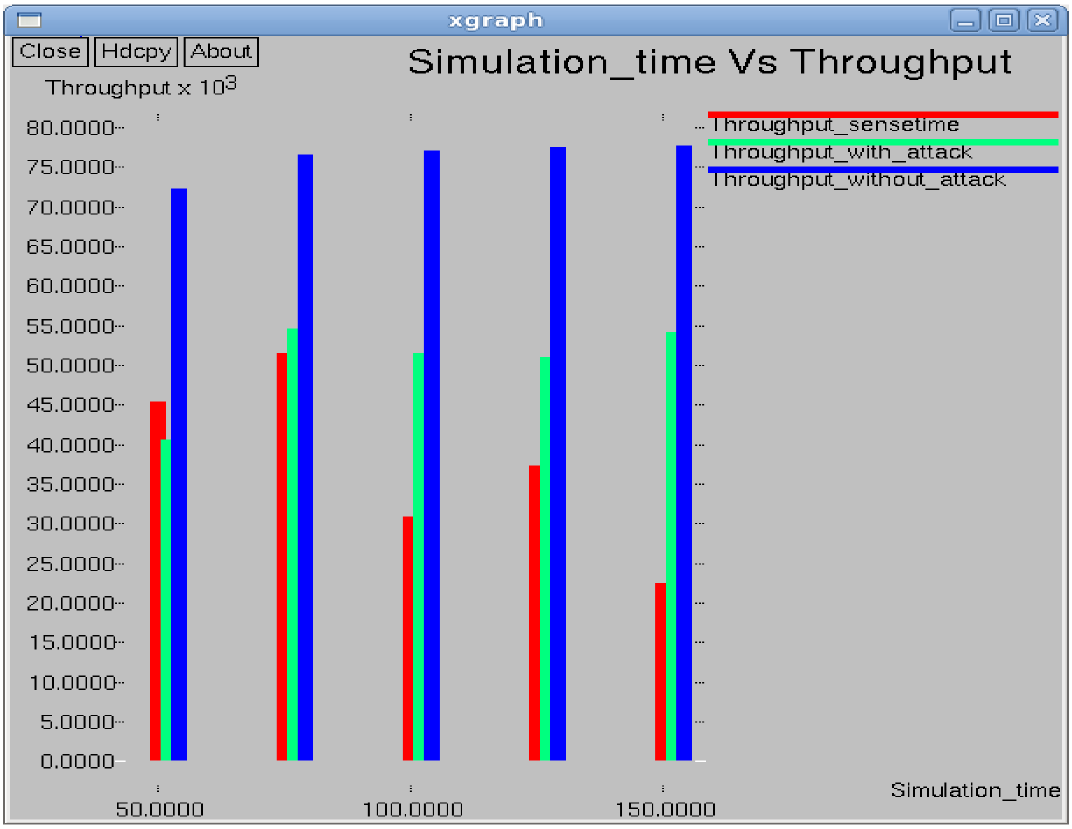

Fig. 2 Simulation time Vs Throughput

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

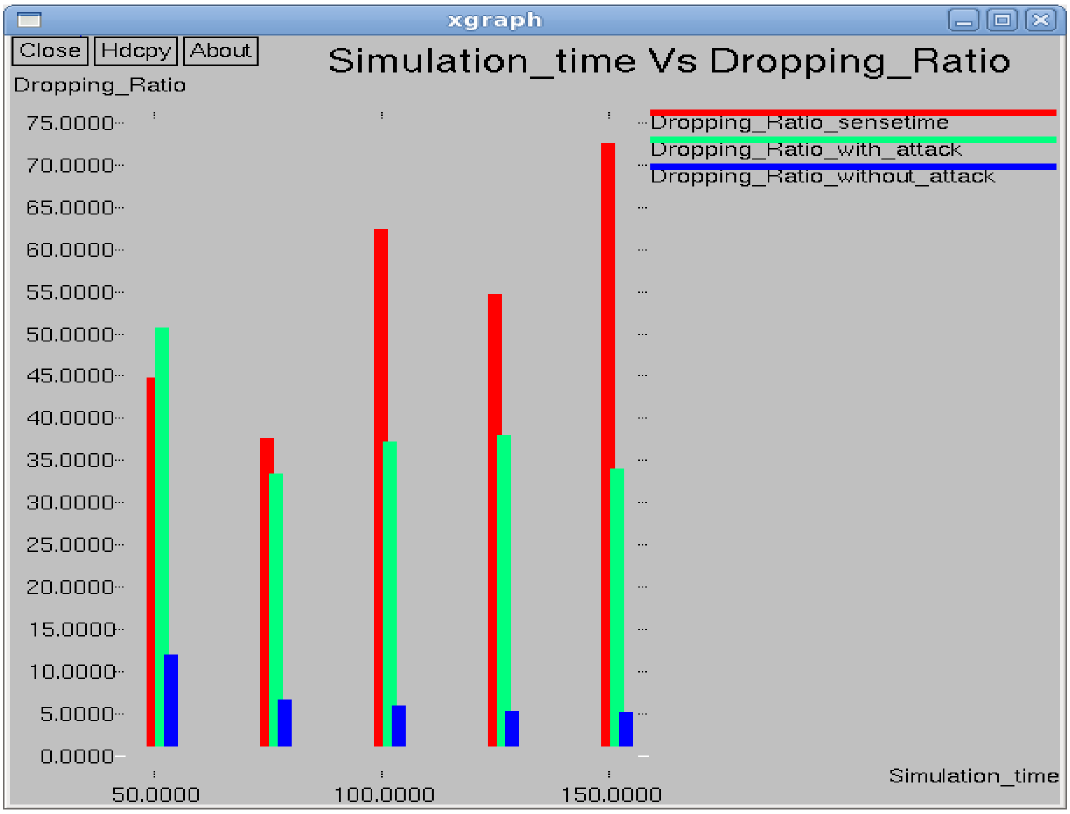

Fig. 3 Simulation time Vs dropping ratio

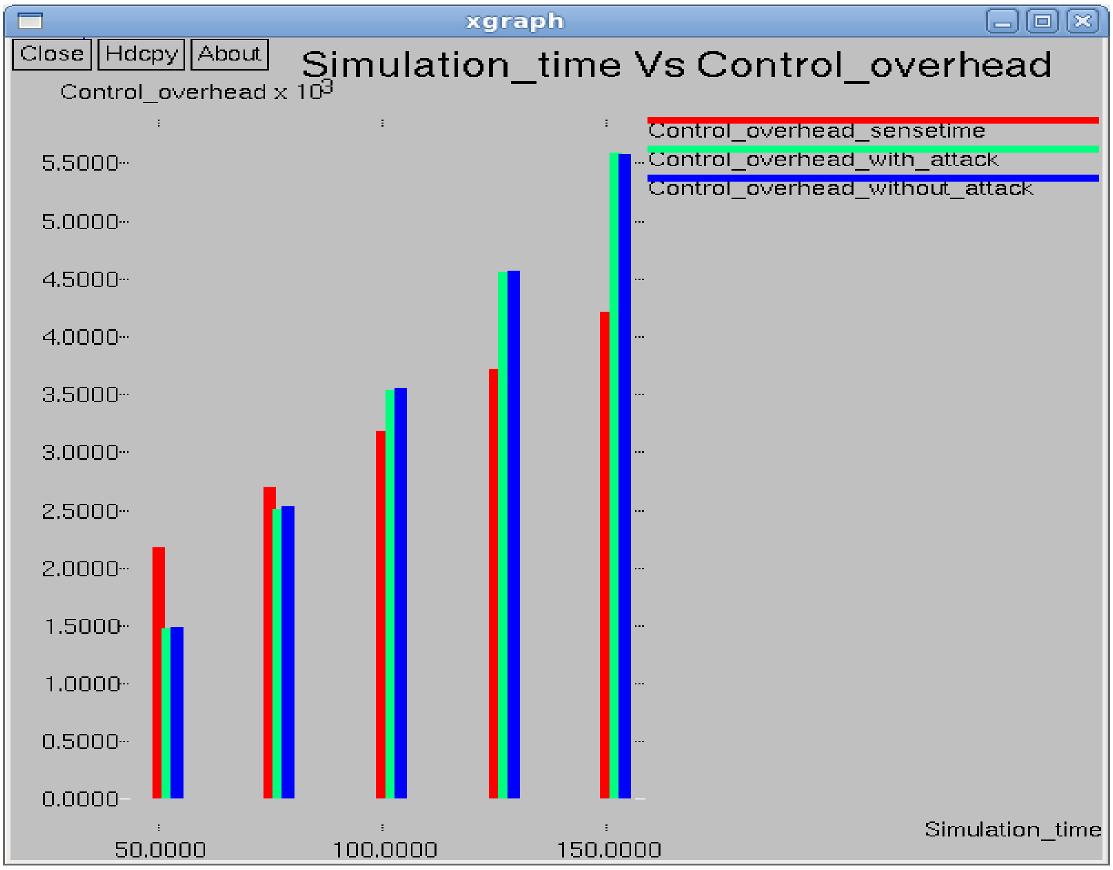

Fig. 4 Simulation time Vs Control Overhead

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

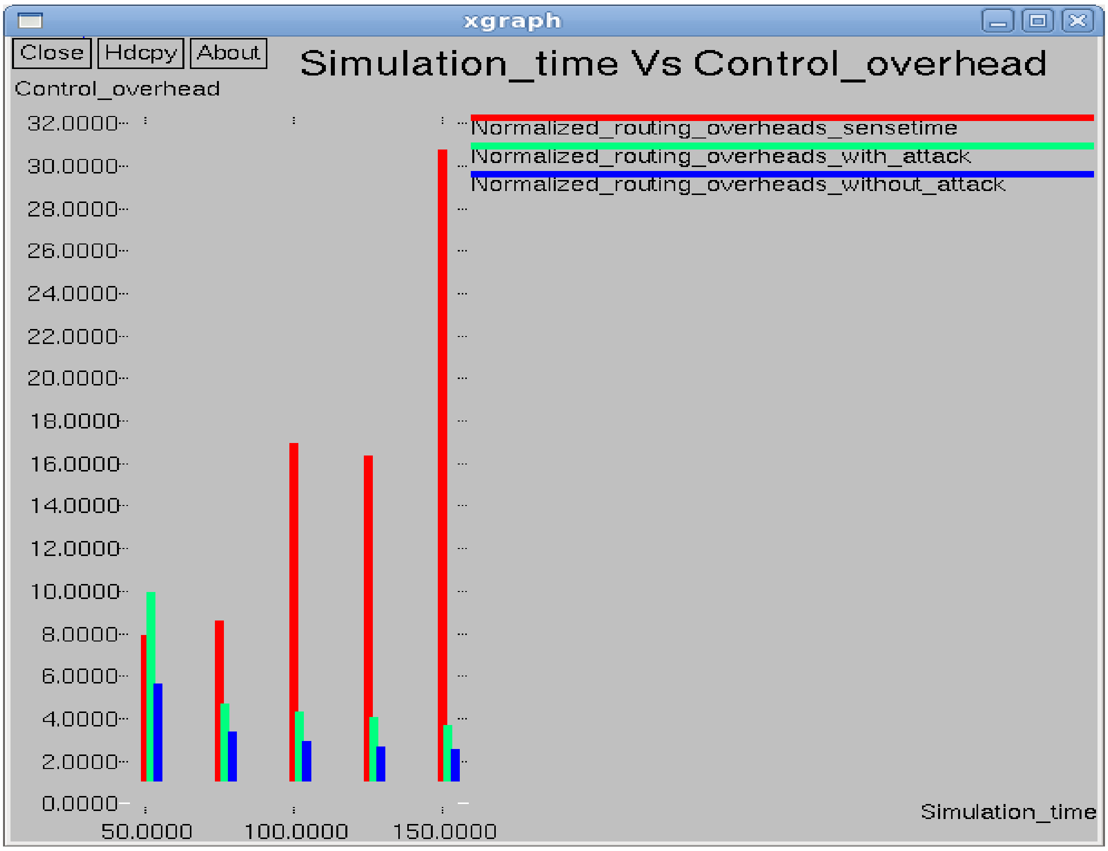

Fig. 5 Simulation time Vs Normalized Routing Overhead

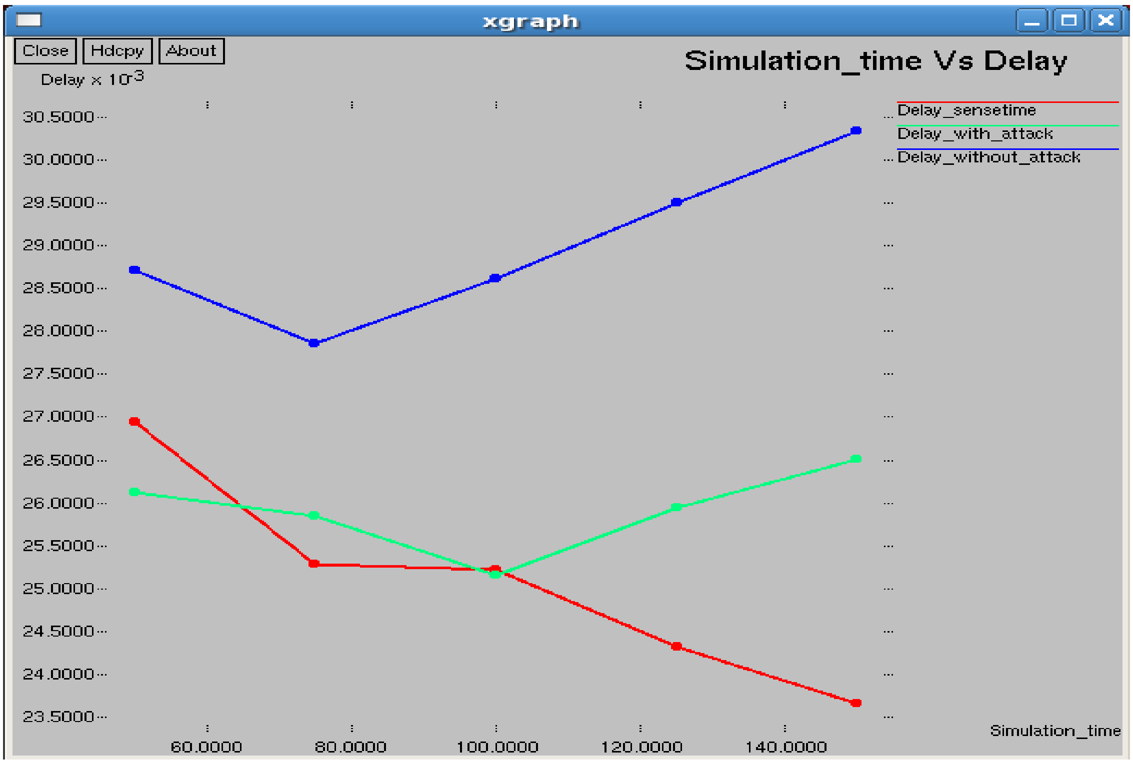

Fig. 6 Simulation time Vs Delay

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

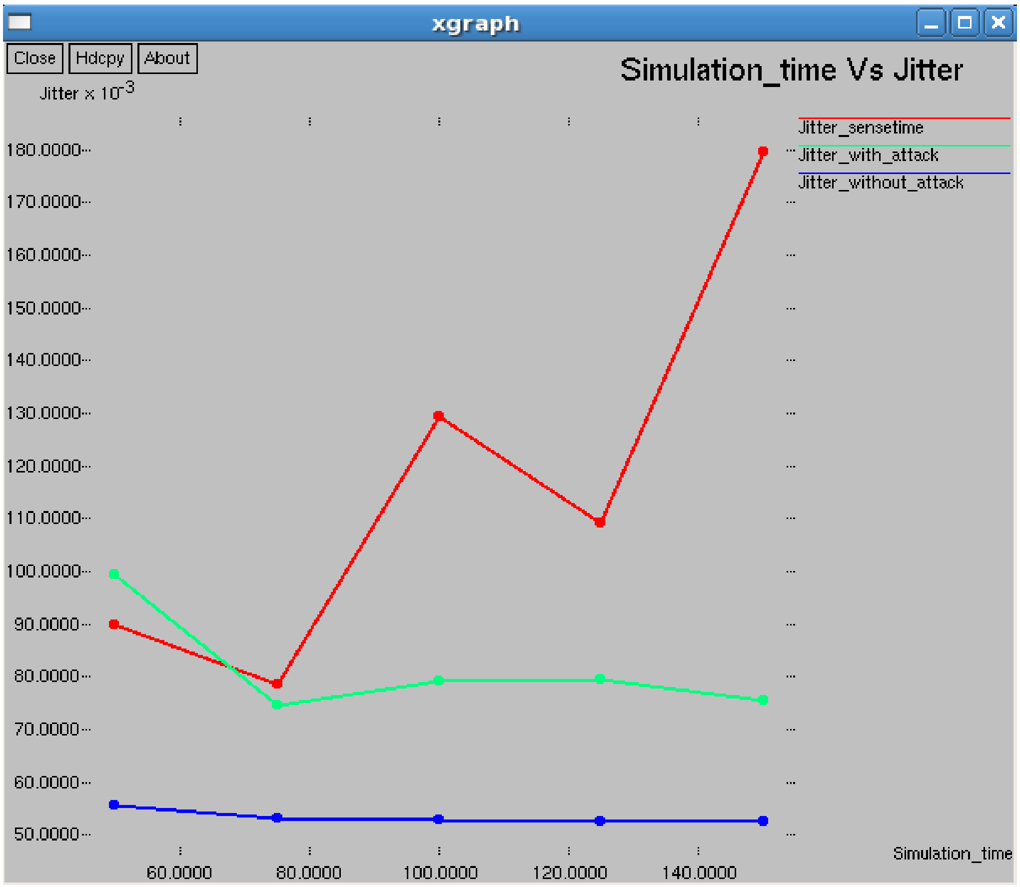

Fig.7 Simulation time Vs Jitter

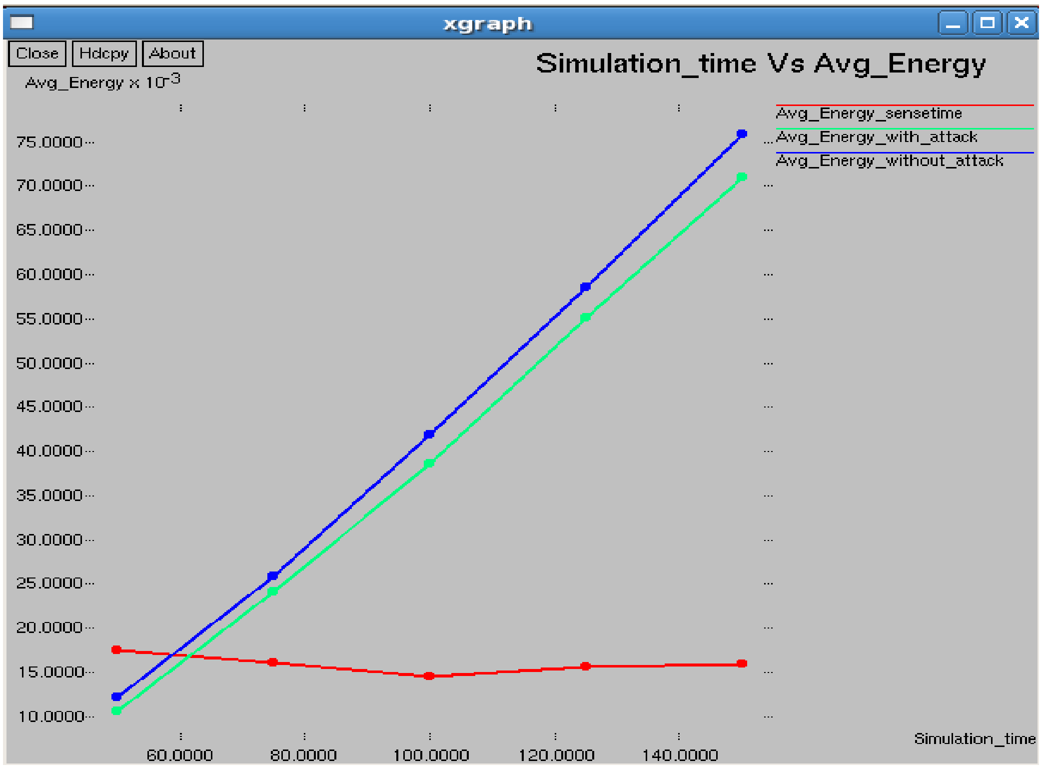

Fig.8 Simulation time Vs Average Energy

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

V CONCLUSION

In this paper we studied the implementation methodology of the TARF. According to that we evaluated the performance results of the various scenarios of the networks. According to the comparison the experimental result shows that as the network scenario changes for the wireless sensor nodes the performance of the network changes in terms of throughput, average energy consumption and other parameters with and without attacker nodes.

ACKNOWLEDGEMENT

It is a pleasure to acknowledge the assistance of my guide **Prof. R. K. Krishna,** Assistant Professor, Department of Electronics and Telecommunication Engineering, R.C.E.R.T, Chandrapur for his valuable guidance, continuous support and advice and constant encouragement throughout my project work. I am also grateful to **Prof. Nitin J. Janwe**, Head, Department of Computer Technology, R.C.E.R.T., Chandrapur for his last minute instructions which helped me to focus my work in the right directions.

I would like to extend my gratitude to honorable **Dr. K. R. Dixit**, Principal, R.C.E.R.T., Chandrapur, for being a constant source of inspiration.

Finally, I would like to extend my thanks to all those who have contributed, directly or indirectly to make this project successful.

REFERENCES

1. J. N. Al-Karaki, A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communication, pp 6-28, December 2004.

2. T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, "Energy efficiency and implementation cost of trust aware routing solutions in WSNs", IEEE Computer Society, 14th Panhellenic Conference on Informatics, pp 194-198, 2010.

3. G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust Aware Routing Framework", IEEE Transactions on Dependable and Secure Computing, Volume: 9 , Issue: 2, 2012.

4. Ms. Dipali Dikondwar, Prof. R. K. Krishna, "Implementation of energy efficient and trust aware routing for WSNs – Energy Consideration", International Journal of Scientific and Engineering Research (IJSER), Vol. 4, Issue 7, ISSN 2229-5518, July, 2013.

5. G. Zhan, W. Shi, and J. Deng, "TARF: A trust aware routing framework for wireless sensor networks", in proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10) 2010.