Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Energy Consumption in Wireless Sensor Network Using Improved Statistical Framework

Sonali Pawar
Department of Computer Engineering,
BSIOTR Wagholi, Pune University,
Pune, India

Prof. Mrs. R. A. Mahajan
Department of Computer Engineering,
Pune BSIOTR Wagholi, Pune University,
Pune, India

Abstract-report by a different application, sensor networks need locations of events for that is to remain anonymous, the unauthorized observers network traffic by analyzing the origin of such events should be unable to detect source known as the anonymity issue, this problem is an important topic in the security of wireless sensor networks as being proposed are based on the assumptions different adversarial techniques has emerged with a variety of proposed Structure innovation is twofold: first, It introduces the notion of "in distinguish ability gaps" and wireless sensor networks; The model provides a quantitative measure of anonymity second, this binary hypothesis testing with nuisance parameters source for statistical problem to oblivion maps. by doing so, we issue the binary code, sample analysis of real valued points the theory study of anonymous sensor networks to be included to change the coding opens the door.

Index terms — wireless sensor networks (WSN &amp ;), source location, privacy, anonymity, hypothesis testing, theory of nuisance parameters, coding.

I. INTRODUCTION

Recently we source into oblivion in a statistical framework for sensor networks towards studied. In most of the reported by a sensor network applications events venues need to remain anonymous. "that is, Unofficial observers network traffic by analyzing such events should be unable to detect the origin of this introduction and the notion of "lag in distinguish ability" model for wireless sensor networks in anonymity provides a quantitative measurement based on assumptions different adversarial techniques with variety of wireless sensor network security; Second, This binary hypothesis testing with nuisance parameters source for statistical problem to oblivion maps how private source information which a extracts the appropriate data changes that reduce the impact of nuisance or information search for exposing to change mapping problem source binary hypothesis testing with anonymity leads to nuisance standards. Transform the problem binary code, Sample analysis of real valued points the theory study of anonymous sensor networks to be included the coding opens the door for the proposed system sensor networks to evaluate the statistical source anonymity proposes a quantitative measure, monitor, and spirit including sensor networks. applications reported interest in a wide range of events are deployed But the military, health care and to keep an eye on the animals, [1], [2], [3] are not limited in time, many applications. Energy-efficient monitoring networks for out of reach is an important feature to create an extended period is expected to operate on energy constrained nodes consist of the monitoring network. In such cases, the nodes only when a relevant event is detected are designed to transmit information (i.e., Event-triggered transmission). As a result, an event-trigger has the location of the node; the location of a real incident report by node can be approximated within range sensing. Varying time intervals to combat vehicle locations on the nodes broadcast can be an enemy to appear.

There are three parameters that an incident is detected and reported by a sensor node can be associated with the description of the event, at the time of the event, and the event location. When sensor networks are deployed in an environment of crooked, three parameters that trigger the transmission a phenomenon can be attributed to protect the privacy of wireless sensor network design is an important safety feature.

Current literature in enemies, namely, local and global enemies fewer than two different types of sources have been addressed the anonymity issue. A local anti-an anti-mobility and network traffic will be limited to partial view is defined. Efficient power saving plan should be developed and appropriate algorithm and the corresponding energy consumption and wireless sensor networks system to improve the lifetime of the network was designed for cluster-based wireless sensor network technology to reduce energy consumption from the point of view is one in this article, We provide efficient energy consumption in the network to optimize energy clustering algorithm proposed. The main idea of this article is uniform clusters conceptual data using transmission sensor nodes in wireless sensor networks in order to reduce distance. In order to make an ideal distribution node cluster for the sensor to, we calculate the average distance between sensor nodes and choosing the appropriate residual energy cluster head nodes to take into account. Wireless sensor networks use uniform lifetime of cluster and network loading is enhanced by balancing among groups. Simulation results in energy consumption and lifetime networks wireless sensor networks to strike appropriate performance for our proposed algorithm indicated by superior performance get.

II. LITERATURE SURVEY

Survey on Wireless Sensor Networks:

A sensor network sensor node, which either event or close it very densely deployed is made up of a large number of sensor nodes position engineer. Be it predetermined or random terrain deployment or disaster relief operations in the other hand, allows. It also means that the sensor network protocols and algorithms must possess self organizing capabilities. Another unique feature of the sensor the sensor network nodes is the cooperative effort sensor nodes are a Board with processor. raw data to nodes instead of sending, responsible for sensor fusion nodes carry out simple computations locally and only transmit the data processed and partly to their processing capabilities Usage.

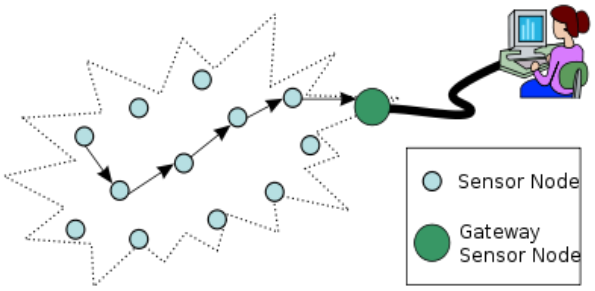


Fig 1: Overview of Sensor Network

The above mentioned features sensor networks to ensure a wide range of applications for some application areas are health, military and safety. For example, a patient about physical data can be remotely monitored by a physician. While this is more convenient for the patient, it is also the doctor to better understand the current condition of the patient allows. sensor networks also air and water in chemical agents detection Can they be used to type, The concentration and location of pollutants can help to identify precisely, sensor network end user intelligence and will provide a better understanding of the environment with us in the future, wireless sensor networks form an integral part of our lives to the present day will be more so than personal computers, imagine.

Realization of these and other sensor network applications that require wireless adhoc networking techniques. Although many protocols and algorithms for wireless ad hoc networks traditionally have been offered, well they have unique features and applications are not suitable for sensor networks requirements. To illustrate this point, sensor networks and ad hoc networks are below the differences between:

1. Sensor is a sensor network node in several orders of magnitude the number of nodes in an ad hoc network can be greater than one.
2. Sensor nodes densely deployed.
3. Sensor nodes are prone to failures.
4. A sensor network topology changes very frequently.
5. The ad hoc networks to communication-based, while the sensor nodes use mainly broadcast communication paradigm.
6. Sensor nodes power, computational capabilities, and memory are limited.
   Sensor nodes global identification (ID) because a large amount of overhead and may not have a large number of sensors

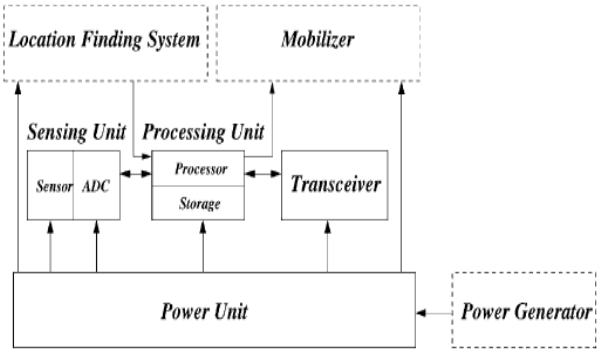


Fig 2: Components of a Sensor Network

Four basic components of a sensor node fig. 2 as shown in the following: a sensing unit, a processing unit, a transceiver unit and a power unit.

They also have a location finding system, a power generator and a dependent may be additional components such as application mobilizes. sensing units are generally made up of two subunits: sensors and analog to digital converters (ADCs) for analog signals, ADC sensor based on observed phenomenon produced by converting the digital signals, and then was fed into the processing unit processing unit, Which usually is associated with a small storage unit, Processes the sensor node to accomplish other tasks assigned sensing nodes are collaborating with a transceiver unit connects to the node network. Of the most important components of a sensor node of one power unit is power unit's power unit such as solar cells can be supported by a cleaning. There are also other subunits which applications are up.

Routing Techniques in Wireless Sensor Networks:

Wireless sensor networks (WSNs) sensing, computing and wireless communication capabilities consist of many small nodes along routing, power management and data dissemination. Protocols where energy awareness essential design issue for WSNs is specifically designed to focus, however, routing protocols which. applications and may differ depending on the network architecture for the paper, We have the State-of-the-art WSNs routing techniques to present a survey we first design challenges separated routing techniques followed by a comprehensive survey of WSNs Routing Protocol framework for the underlying network infrastructure, routing technology. Overall, based on are classified into three categories:

1. Flat
2. Hierarchical
3. location-based routing.

In addition, these protocols in multipath-based query-based, negotiation-based QoS-based and coherent-based protocols can be classified on the basis of the operation.

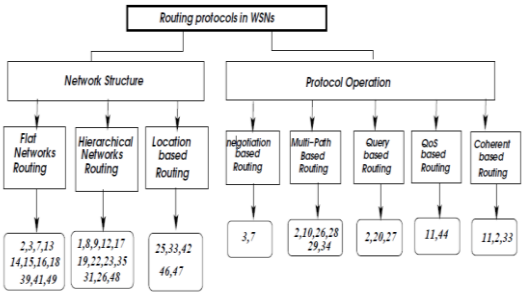


Fig 3: Routing Protocols in WSN

- Many researchers to source anonymity in sensor networks towards a statistical framework is a qualitative and quantitative analysis
- I. Akyildiz, w. Su, y. Sankarasubramaniam, and e. Cayirci, [1] in this paper resilience, fault tolerance, high-fidelity characteristics sensing, low cost and rapid deployment sensor networks of remote sensing to create many new and exciting application areas. In the future, the wide range of application areas form an integral part of our lives wills sensor networks. However, realization of requirements sensors fault tolerance, Scalability, cost, hardware, topology changes, Environment and power consumption as factors to satisfy the constraints introduced by these network constraints are extremely stringent and sensor networks for wireless adhoc networking, since new technologies are required.
- Arampatzis, j. Lygeros and Manesis, [2] this paper wireless sensors and wireless sensor networks in the scientific community have come to the forefront lately. It enables many applications engineering is the result of increasingly small size devices, use these sensors and the possibility of organizing the network has revealed a number of issues dealing with research and new approaches to certain issues that are highlighted in this paper. Where such a sensor network access has been proposed in various application areas are surveyed.
- J. Yuck, b. Mukherjee, and d. Ghostly, [3] this paper a wireless sensor networks (WSN &) in critical applications such as remote environmental monitoring and tracking the target is small, cheap, and intelligent sensor, especially of recent years, have been enabled by the availability of these sensors wireless interface with which they are with one another can communicate as a network are equipped with a design of WSN & much depends on application, And this environment, application design goals, costs, hardware, and systems must consider factors such as the lack of.
- Y. Xi, L. Schwiebert, and W. Shi [4] in this paper a wireless sensor network is deployed to monitor certain events and pinpoint their locations, the location information is intended only for legitimate users. However, an eavesdropper can monitor the traffic and deduce the approximate location of monitored objects in certain situations. We first describe a successful attack against the flooding-based phantom routing, proposed in the seminal work by Cell Ozturk, Yongyong Zhang, and Wade Trappe. Then, we propose GROW (Greedy Random Walk), a two-way random walk, i.e., from both source and sink, to reduce the chance an eavesdropper can collect the location information. We improve the delivery rate by using local broadcasting and greedy forwarding. Privacy protection is verified under a backtracking attack model.
- B. Hoh and M. Gruteser, [5] in this paper prevalence of sophisticated location-tracking and wireless communication technology gives rise to a novel class of application that gather statistical information about people's movements. Current data perturbation techniques are unable to protect time-series location information. We have proposed a data perturbation technique that increases path confusion by slightly modifying reported positions for two users that are in close proximity of each other. This technique can limit the tracking duration, for which an adversary can follow an individual user. Specifically, we conclude that the Path Perturbation algorithm improves privacy with a lower mean location error that means at a lower quality of service penalty than a Gaussian perturbation algorithm. the Path Perturbation algorithms achieve promising results in an environment with about 10 vehicles per square mile, which is a user density targeted in traffic monitoring applications.

III. IMPLEMENTATION DETAILS

The system infrastructure consists of a BS and a few sensor nodes we head non-censored in all nodes of the cluster nodes to categorize and head nodes cluster. Non-cluster head nodes environment information is to monitor and transmit data from the cluster head node sensing mode work. In addition, sensors to gather data from a cluster node becomes the head it compresses and cluster head mode forwards to BS. System structure is shown in the figures of this article.

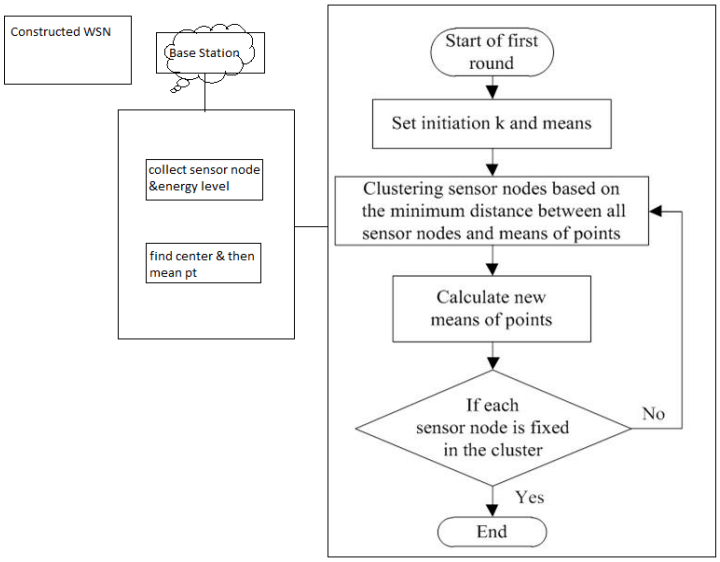


Fig 9: System Overview

Energy efficiency increase and sensor nodes in wireless sensor networks to extend the lifetime of efficient power saving has created and developed the algorithm clustering architecture is based on should be centralized, we better wireless sensor network lifetime network and efficient energy consumption to provide a proposed plan of OECA., We think the BS and get information for each sensor node residual energy and can calculate average residual energy when the average residual energy sensor node is more than residual energy, sensor node cluster becomes a candidate we head sensor node cluster is an ideal distribution for all sensor nodes [12, 13] location and residual energy use information to create k-means algorithm, modify the algorithm includes two phases in operation: steady-state and set up steps.

3.1 System Features:

The reason the network traffic to reduce the amount of broadcasting fake events, for node-based technologies and data aggregation behind the scenes have been proposed. such techniques, behind the scenes the intermediate nodes that act as filters out duplicate messages or multiple messages in a single transmission overall is less overall communication overhead by a high communications overhead such approaches. Reducing the issue by generating fake messages more attractive make plans based on.

3.2 Algorithm Used:

Existing Algorithms:

1. HEED

1. Cluster head selection
2. Hybrid of residual energy (primary) and communication cost (secondary) such as node proximity
3. Number of rounds of iterations
4. Tentative CHs formed
5. Final CH until $CH_{prob}=1$
6. Same or different power levels used for intra cluster communication.

2. Letch

Minimum Transmission Energy (MTE) for 3 nodes A, B and C, A would transmit to node C through B if (E_{tM} – total transmit energy)

Et_M (kid=d_{ab}) + E_{tM} (kid=d_{ca}) < E_{tM} (Kod_{ak})

B to C to A and B power transmission A less transmission power nodes to node C then B would be elected as the intermediate node.

MTE nodes are in which BS is nearby to quickly and who will die from distant nodes.

Other intermediate nodes have nodes more than energy consumption as used.

Wireless sensor networks, data communications to consume a large amount of energy. Total energy consumption average by non-cluster head nodes and the cluster head nodes are data transmission of dissipated energy. In addition, data collection and the cluster head nodes to stockpiling of energy consumption is considered.

E_{tM} (Led) = E_{lect} * L * a_{mp} * L

E_r (L) =E_{lect} * L

Where d is the distance between the two sensor nodes, E_{tM} (Led) is the transmitter energy consumption, and E_{RX} (L) is the receiver energy consumption. E_{lect} is the electronics energy consumption per bit in the transmitter and receiver sensor nodes. Amp is the amplifier energy consumption in transmitter sensor nodes, which can be calculated by

$$\varepsilon_{amp} = \begin{cases} \varepsilon_{fs} * d^2, \text{ when } d \leq d_0 \\ \varepsilon_{mp} * d^4, \text{ when } d > d_0 \end{cases}$$

Where d_0 is a threshold value, if the distance d is less than d_0, the free-space propagation model is used. Otherwise, the multipath fading channel model is used. Fsg and a_{mp} are communication energy parameters.

Only consider transmitter energy, neglects energy dissipation of the receivers

3. K Means

Use of k-means algorithm to partition the n sensor nodes into k clusters in which each sensor node belongs to the cluster with the nearest mean of point, If there are k clusters in the system, the k-means function can be expressed by

Avgs $\sum_{i=1}^{k} \sum_{Xj \in Si} | X_j - m_i |^2$

Where Si is the cluster i, X_k is coordinate of sensor node j and mi is the coordinate of mean of point.

3.3 Proposed Work

The paper writer during binary hypothesis testing for modeling, analysis, and evaluation of the statistical source anonymity in wireless sensor networks based on a statistical framework provided in the framework which it presented letters. Consists of:

1) proposed the introduction of the notion of "indistinguish ability interval" method and model for wireless sensor networks in anonymity provides a quantitative measurement;

2) The proposed method is tested with nuisance parameters source anonymity binary hypothesis statistical problem then anonymous map sensor networks using the proposed model designed to analyze the existing solution.

According to the results in the paper, the proposed approach to improve their anonymity against correlation for showing the possible amendment to the tests.

However they are still likely to improve efficiency of the proposed approach therefore in this project we have to satisfy the notion of indistinguish ability interval mechanism to extend the existing base by adding paper method are going to.

Proposed Algorithm:

Initiate(s);
While (Receive Nu (.) from u) && (Ns (.) is not stable) do
For each vertex d ∈ V/{s} do
S orders its M neighbors by NBs (1) (d) ≤… ≤
NBs (M) (d).
Ns: = Ns0 (d) and FLs: = FLs0 (d);
For each neighbor Bs (i), i: = 1, M do
If Ns > NBs (i) (d) then
If N (merge {FLBs (i) (d), FLs}) ≤
N ({s, FLBs (i) (d)})
Then
Ns: = N (merge {FLBs (i) (d), FLs});
FLs: = merge {FLBs (i) (d), FLs};
Else
Ns: = N ({s, FLBs (i) (d)}), FLs: =
{S, FLBs (i) (d)};
Send FLs (.) and Ns (.) out.

3.4 Mathematical Model:

1. Correlation Measure for Binary Hypothesis Testing

In this section, we specify the statistical measure that will be used to perform our experimental analysis of SSA approaches based statistical goodness of fit tests.

Let X={x1, xn} and Y= {y1, yn} be two sequences of length n. Define the correlation coefficient of the two sequences by

$$\rho(X,Y) = \frac{\left| n\sum_{i=1}^{n} x_i y_i - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right) \right|}{\sqrt{\left(n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2\right)\left(n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2\right)}}$$

IV. RESULTS

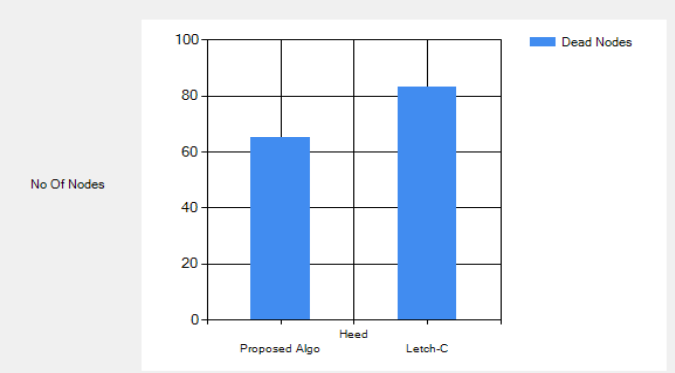
4.1 Hardware and Software Used

Hardware Configuration:
-PROCESSOR : PENTIUM IV 2.6 GHz
-RAM : 512 MB DD RAM

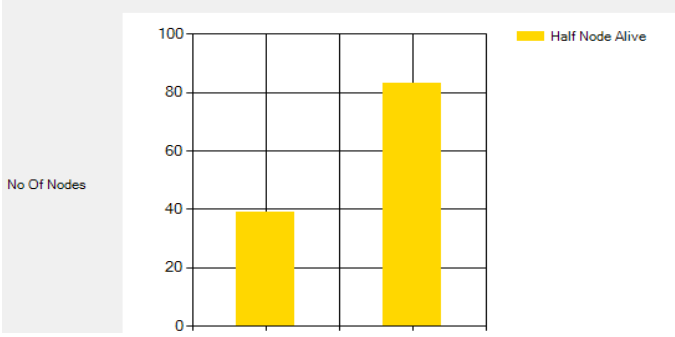
-MONITOR : 15" COLOR
-HARD DISK : 20 GB
Software Configuration:
-Front End : C#.Net
-Tools Used : VS2010
-Operating System: Windows XP/7

4.2 Result of Practical Work:

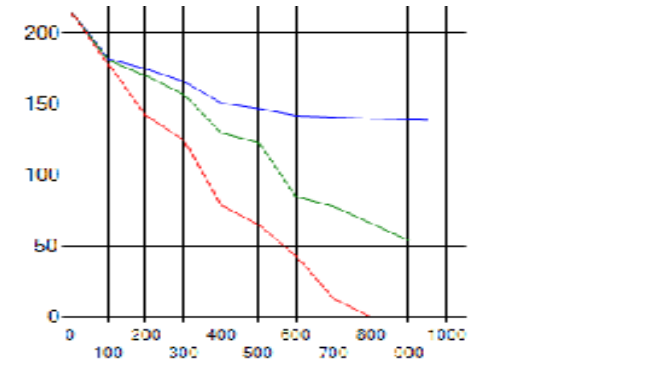
4.2.1 Dead Node info:



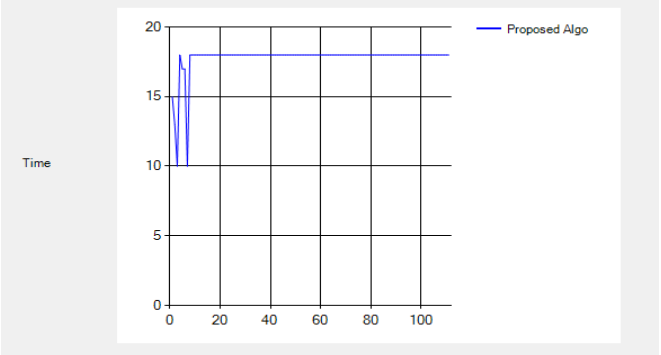
4.2.2 Half Alive Info:



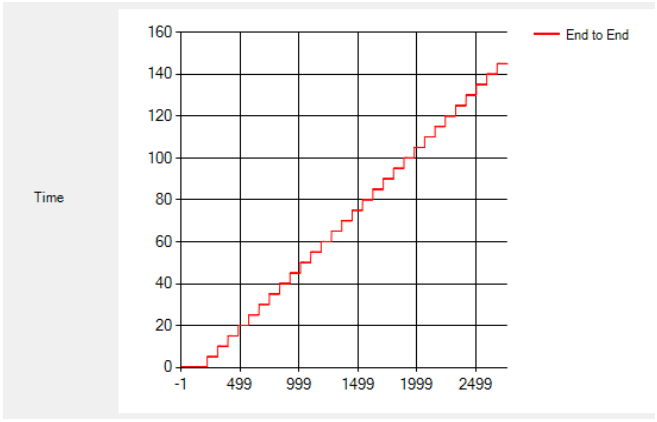
4.2.3Total Energy:



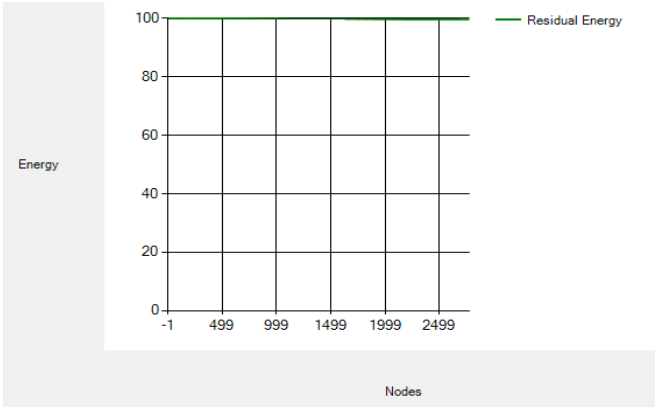
4.2.4 Energy Efficiency:



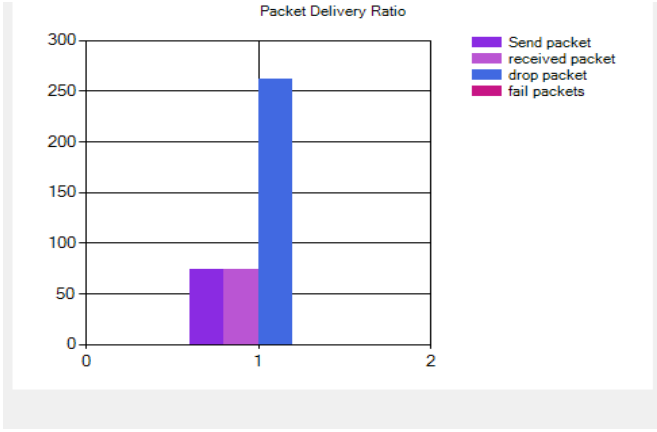
4.2.5 End to End Delay



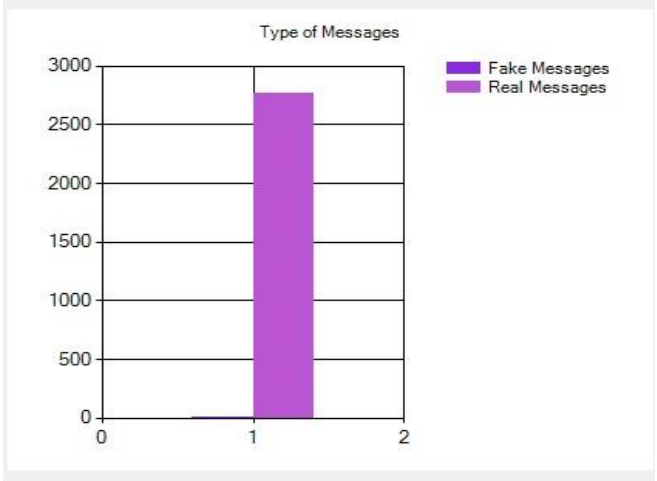
4.2.6 Residual Energy:



4.2.7 Packet Ratio:



4.2.8 Packet:



V. CONCLUSION

In this project, we have a statistical framework for modeling binary hypothesis testing, analysis, and evaluation of the statistical source anonymity in wireless sensor networks based on provided we model source location privacy gaps introduced the concept of indistinguish ability. We revealed that are uncorrelated, faux intervals while the anonymous statistical systems designed to introduce in the current approach to correlation real intervals. binary source of nuisance parameters with information hypothesis testing statistics problem to explore the problem of matching, we found out why previous studies performed in this paper had been unable to locate the source of the information leak was finally We present solutions to improve their anonymity against correlation tests for proposed an amendment.

REFERENCES

Base Paper: Basel Alomair, Member, IEEE, Andrew Clark, Student Member, IEEE, Jorge Cuellar, and Radha Poovendran, Senior Member, IEEE: **Toward a Statistical Framework for Source Anonymity in Sensor Networks.**

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," Proc. IEEE 13th Mediterranean Conf. Control and Automation (MED '05), pp. 719-724, 2006.

[3] J. Yuck, B. Mukherjee, and D. Ghostly, "Wireless Sensor Network Survey," Computer Networks, vol. 52, no. 12, pp. 2292-2330, 2008

[4] Y. Xi, L. Schwiebert, and W. Shi, "Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks," Proc. IEEE 20th Int'l Parallel & Distributed Processing Symp. (IPDPS '06), pp. 1-8, 2006.

[5] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," Proc. IEEE/Created First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05), pp. 194-205, 2005.

[6] N. Li, N. Zhang, S. Das, and B. Thuraisingham, "Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey," Elsevier J. Ad Hoc Networks, vol. 7, no. 8, pp. 1501-1514, 2009.

[7] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 28, no. 5, pp. 677- 691, June 2010.

[8] C. Jacque and A. Bera, "A Test for Normality of Observations and Regression Residuals," Int'l Statistical Rev. /Revue International de Statistique, vol. 55, no. 2, pp. 163-172, 1987.

[9] Y. Jiang, Y. Fan, X. Shen, and C. Lin, "A Self-Adaptive Probabilistic Packet Filtering Scheme against Entropy Attacks in Network Coding," Computer Networks, vol. 53, no. 18, pp. 3089- 3101, 2009.

[10] W. Yang and W. Zhu, "Protecting Source Location Privacy in Wireless Sensor Networks with Data Aggregation," Proc. Seventh Int'l Conf. Ubiquitous Intelligence and Computing (UIC '10), pp. 252- 266, 2010.

