Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Approaches for Mitigating Replica Nodes in WSN

S.Kumaravel
HOD, Computer Science,
Mahendra Arts and Science College,
Kalippatti, Namakkal, India

Dr.M.Karthikeyan
HOD, Computer Science,
K.K. College
P.velur, Namakkal, India

S. Prabha
Assistant Professor
Muthayammal Engg. College
Raspipuram, Namakkal, India

Abstract*— *A WSN is composed of a large number of tiny sensor nodes and one or multiple more powerful sink nodes. Sensor nodes collect data from the surrounding environment and distribute the collected data to a sink node. Every sensor node has one or more sensors, a general purpose Central Processing Unit (CPU) to perform arithmetic and logical operations, and a small amount of storage space. The power is supplied to these sensor nodes through minute, non-replenish able batteries. A sensor node has a wireless communication interface during which it can communicate with other nodes in its locality. Recent works carried out, considers Energy Efficient Finite Range Query [FRQ] Scheme in a wireless sensor network which provides an efficient method to identify the mobile replica nodes and eliminate the varying query ranges of mobile sensor nodes. The proposal of the work proceeds in a direction of extending replica detection scheme of probability ratio test with Finite Range Query (FRQ) technique. This technique discovers the mobile replica nodes which is acting as an adversary and remove the query range variations of mobile sensor nodes and also the FRQ technique improves energy efficiency of the sensor nodes by reducing the message query transmission on data aggregation. But it is necessary to validate the query to improve the detection of mobile replica nodes in a wireless sensor network. For this purpose, in this proposed work presents a novel framework; Deployment of Query Validation for Finite Range Query [DQV-FRQ] mechanism is developed in sensor network. DQV-FRQ presented Query validation scheme to validate the query and to improve the detection of mobile replica nodes. Next work Alternate Traffic Data Control Scheme [ATDCS] in a wireless sensor network is considered to manage the packet creation rate at the sources and transitional nodes in a wireless sensor network. Adaptive Traffic Data Control scheme avoids over-utilizing the network in terms of the node packet buffers and wireless channels. It enhances the data transmission between the sink and the base station and control the packet generation rate at the sinks and intermediary nodes. Performance of ATDCS Framework is evaluated by the number of metrics such as energy efficiency, finite range query, bandwidth, adversary replica nodes, delay, reliability, data loss, traffic control rate, scalability and mean packet generation rate.

Keywords*— *Replica nodes, WSN, FRQ, DQV-FRQ, ATDCS

I. INTRODUCTION

A. Wireless Sensor Network

A budding technology which has established a major attention from the research community is incorporated in the wireless sensor networks. Several small and low-cost devices are comprised in the sensor networks that are self-organizing ad-hoc systems. They view the physical surroundings gather the information and broadcast it to one or more sink nodes. Usually, the radio broadcasts range the sensor nodes in the order of magnitude smaller than the geographical extent of the entire network.

Therefore, data should be transmitted towards the sink node hop-by-hop in a multi-hop manner. By dropping the amount of data which requires to be transmitted, the energy consumption of the network can also be condensed. A huge number of little electromechanical devices with sensing, computing and communication capability are comprised in the wireless sensor networks. They can be used for collecting sensory information, such as temperature capacity, from a wide-ranging geographic area.

In this proposed work uses the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. Sensor networks can consist of hundreds or thousands of low-power, low-cost nodes, most likely movable but more likely at fixed locations, deployed en masse to observe and influence the environment. The possible uses of the sensor networks have been researched vigorously. Some demanding issues are formed owing to the individuality of the wireless sensor networks. The following individuality is mostly focused:

- Sensor nodes tend to fail.
- Sensor nodes make use of a broadcast communication model and have brutal bandwidth constraints.
- Sensor nodes have inadequate resources.

B. Attacks on Sensor Network Routing

A lot of sensor network routing protocols are relatively easy, and for this cause are occasionally even more vulnerable to attacks beside general ad-hoc routing protocols. Most network layer attacks beside sensor networks drop into one of the following categories:

Spoofed, altered, or replayed routing information

- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

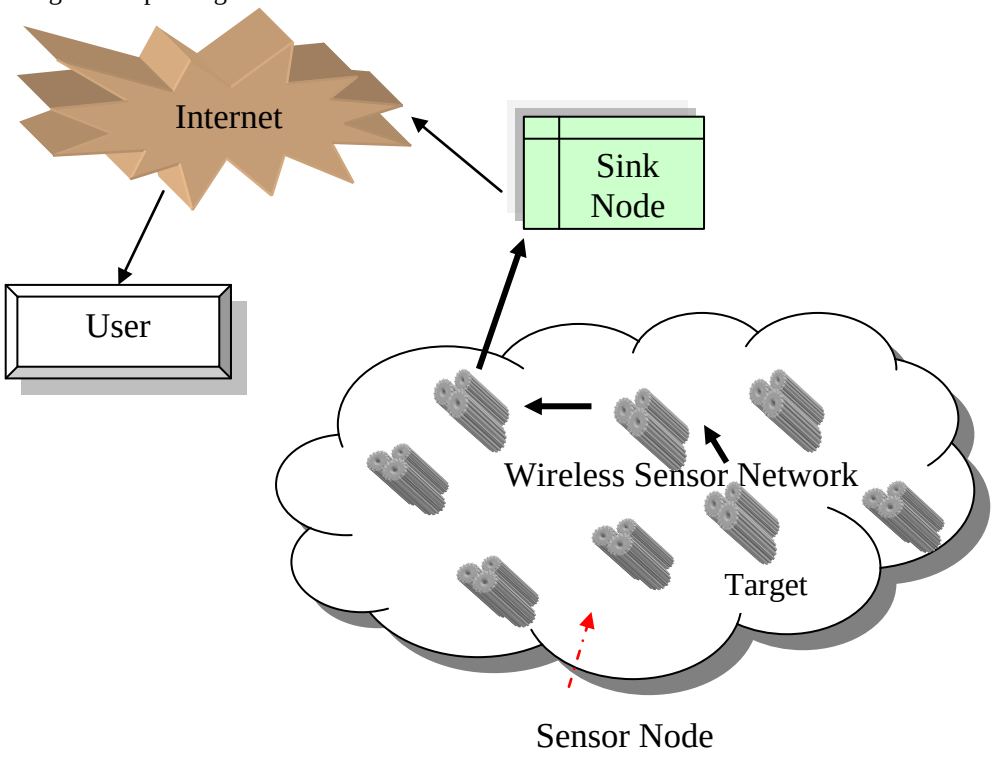

Fig 1 Wireless Sensor Network

Wireless networks are fetching more trendy and it is used in all genuine world applications. So it is required to present a good query ranging method to detect adversary attacks in the wireless sensor networks. Numerous attacks are generated by the attackers to receive the valuable information from the network. In turn, it sends to the adversaries and at the same time transmits inappropriate message to the sink in the sensor networks. This intends to decline the security of the information.

To progress the existence of the network by detecting the attackers and to remove the query range variations which reduces the message query transmission on data aggregation. Energy Efficient Finite Range Query Scheme (FRQ) is presented here to perform a random walk with two limits in such a way that every walk is determined by the experimented speed of a mobile node to detect the mobile adversary attack. This technique minimizes the message query transmission, eradicates the varying query ranges of mobile sensor nodes and improves the security.

But in the Wireless sensor Network query validation plays an important role. Deployment of Query Validation for Finite Range Query [DQV-FRQ] mechanism is developed to validate the query and to improve the detection of mobile replica nodes. By validating the query in wireless sensor networks, the mobile replica nodes are removed entirely and it reduces the loss of data occurred while transaction between the nodes in the network environment. To overcome the over-utilization of network in terms of the node packet buffers and wireless channels, Adaptive Traffic Data Control Scheme [ATDCS] is considered. It enhances the data transmission between the sink and the base station to control the packet generation rate at the sinks and intermediary nodes.

II. LITERATURE REVIEW

In wireless sensor networks, sensor nodes are typically fixed to their locations after deployment. Conversely, an attacker who compromises a subset of the nodes does not require standing for same limitation. If the attacker moves his compromised nodes to numerous locations in the network, such as by employing simple robotic platforms or affecting the nodes by hand, evade schemes that attempt to use location to find the source of attacks. In performing DDoS and false data injection attacks, it takes advantage of diversifying the attack paths with mobile malicious nodes to avoid network-level defences.

For attacks that disturb or undermine network protocols like routing and clustering, touching the misbehaving nodes prevents them from being easily identified and blocked. Thus, mobile malicious node attacks are very dangerous and need to be detected as soon as likely to reduce the harm they can cause. Jun-Won Hoa., et al., 2011 first identifies the problem of mobile malicious node attacks, and explain the limits of a variety of naive measures that might be used to discontinue them. To defeat these limitations, suggest a scheme for distributed detection of mobile malicious node attacks in static sensor networks.

The key thought of this scheme is to relate sequential hypothesis testing to find out nodes that are silent for unusually many time periods such nodes are likely to be moving and block them from communicating. By performing all detection and blocking locally, keep energy consumption overhead to a minimum and keep the cost high. During analysis and simulation, demonstrate that the proposed scheme achieves fast, effective, and robust mobile malicious node detection ability with reasonable overhead.

Storing data on sensor nodes at a particular location is a helpful technique for data-centric storage and organization of location dependent data on wireless sensor networks. To reduce the cost of accessing these data, arranging replicas of data so that the distance between the consumer nodes and replica holder nodes decreases is desirable. Conventional schemes, though, are expensive for updating the replicas still if they are not frequently used or do not hold up functions for ensuring their constancy. Ishihara, S., and Suda, T., 2009 propose a novel replica arrangement scheme, which adaptively arranges replicas at positions close to nodes for recurrent transfer of queries.

Instead of arranging many replicas on sensor nodes, the plan consists of nodes with pointers that point to the replica holder nodes in order to save storage for replicas. The pointers, which are lesser than replicas, are arranged so that the nodes are in circular arcs surrounding the location where the original data item is connected. Simulation results show that the scheme outperforms conventional replica arrangement schemes in terms of the cost necessary for sending queries and replies with adequately low replica update cost.

Chia-Mu Yu., et al., 2009 explains the challenging problem of node replication detection. Although defending against node replication attacks demands immediate attention, only a few solutions were proposed. In this paper, an Efficient and Distributed Detection (EDD) scheme and its variant, SEDD, are proposed to oppose against node replication attacks in mobile sensor networks. The characteristics overcome by EDD and SEDD include (1) Distributed Detection; (2) Efficiency and Effectiveness; (3) Individual Detection; (4) Network-Wide Revocation Avoidance. Performance comparison with recognized methods is provided to exhibit the efficiency of the EDD and SEDD schemes.

The advanced sensor network architectures might be used for a diversity of applications including intruder detection, border monitoring, and military patrols. In potentially hostile environments, the safety of unattended mobile nodes is tremendously critical. Due to the unattended nature of wireless sensor networks, an opponent can capture and compromise sensor nodes, make replicas of them, and then increase a diversity of attacks with these replicas. These replica node attacks are hazardous since they allow the attacker to influence the compromise of a few nodes to apply control over much of the network.

Numerous replica node detection schemes have been proposed in the literature to protect against such attacks in static sensor networks by D. Prabhakaran., et al., 2011. However, these schemes rely on fixed sensor locations and therefore do not work in mobile sensor networks, where sensors are predictable to shift. In this work, a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test is completed. Jun-Won Ho., et al., 2009 propose a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test. To the best of the knowledge, this is the first work to undertake the problem of replica node attacks in mobile sensor networks. Show systematically and during simulation experiments that the scheme provides effectual and vigorous replica detection capability with sensible overheads.

There have been various methods studied to develop a Finite range query scheme in wireless sensor network. They apply the random way point model to detect the replica node attacks by eliminate the varying query ranges and minimizing the message query transmission.

Even though energy efficient Finite range Query Scheme provides an efficient method to detect the adversary attacks but validate the query in wireless sensor network is not achieved. To enhance the query validation, in this work, presents a new approach named Deployment of Query Validation to improve the detection of mobile replica nodes.

Some techniques have been developed for providing security in the sensor network by validating the query. The main concern is that it cannot supply an end to end secure communication in the conventional environment.

Another technique for the validating query is that generating a scheduling plan to target the user interested data in Multi-region Query technique. The anxiety is that the query is not fetched with minimum latency to satisfy the user. The current query validation method is incomplete, if any, various unwanted effects that defeat the objectives of the sensor network, Adversary attacks is much more vulnerable to malicious exploits than a wired network. Secure communication without any failure is an important aspect of any network environment.

One work designed is that CS-REC can achieve the recovery performance close to the case where there is no data loss. The compressive sensing (CS) with real expander codes (RECs), coined as CS-REC, for robust data transmission but the traffic load is not balanced for specific source destination pairs.

Fuzzy Energy Aware tree-based Routing (FEAR) protocol that aims to enhance existing tree-based routing protocols and prolong the network's life time by considering sensors' limited energy but the management of packet creation rate and transiting nodes fails. To enhance the packet creation rate at the sink, plan to devise an adaptive traffic data control mechanism.

III. ENERGY EFFICIENT FINITE RANGE QUERY SCHEME FOR DETECTING MOBILE ADVERSARY REPLICA NODES IN WIRELESS SENSOR NETWORKS

Due to the unattended nature of wireless sensor networks, an opponent can detain and cooperation sensor nodes, produce replicas of those nodes, and increase a diversity of attacks with the replicas he injects into the network. These attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to apply control over much of the network. Numerous replica node detection schemes in the literature have been intended to defend beside these attacks in static sensor networks. These approaches rely on fixed sensor locations and consequently do not work in mobile sensor networks, where sensors are conventional to move.

In sensor networks, adversaries may effortlessly detain and compromise sensors and organize a limitless number of clones of the compromised nodes. Since these clones have legitimate access to the network (legitimate IDs, keys, other security credentials, etc.), they can contribute to the network operations in the similar way as a legitimate node, and therefore begin a huge variety of insider attacks, or still take over the network. If these clones are left unnoticed, the network is undefended to attackers and thus tremendously susceptible.

Therefore, clone attackers are rigorously critical and effective and efficient solutions for clone attack discovery want to limit their damage. However, detecting cloned attacks is not unimportant at all. The primary challenge comes from the fact that the replicas own all the security information (ID, keys, codes, etc.) of the unique compromised sensor. Thus, they can pass all the identity/security check and run away from being distinguished from a legitimate sensor.

In addition, a "smart" clone may attempt to conceal from being detected by all means. In addition, clones may conspire to deceive the network administrator into believing that they are genuine. Note that an opponent may allocate clone nodes everywhere in the network. Thus localized detection schemes do not work competently.

Proposed technique, the replica detection scheme of probability ratio test with Finite Range Query (FRQ) is to detect replica node attacks in mobile sensor networks. In static sensor networks, a sensor node is experiential as being simulated if it is situated in more than one place. If nodes are touching approximately in the network, although, this technique does not work, because a benevolent mobile node will be treated as a replica because of its incessant change in location.

Therefore, use some other method to identify replica nodes in mobile sensor networks. Providentially, mobility offers us with an evidence to assist resolve the mobile replica discovery problem. Propose a mobile replica detection scheme by leveraging this intuition. The architecture diagram of the Energy Efficient Finite Range Query Scheme is shown in Fig. 2.

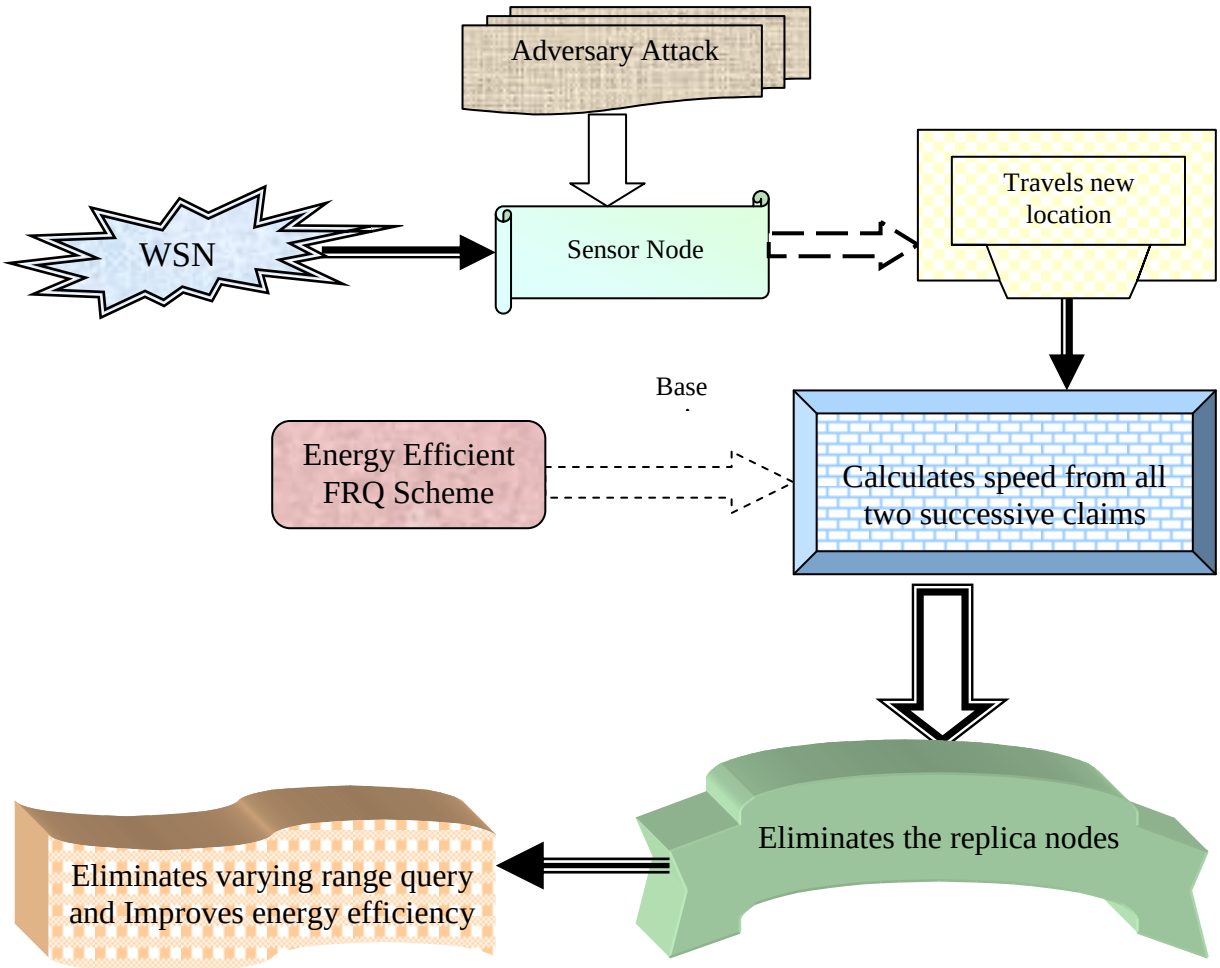

Fig 2 Energy Efficient FRQ Scheme

In the above architecture diagram, the wireless sensor network senses the node and finds the adversary attack. The sensed nodes are travelling during new position. It calculates the speed from all two successive claims through Energy Efficient Finite Range Query scheme. The calculated speed eliminates replica nodes and improves the energy efficiency in the wireless sensor network.

Proposed Energy Efficient Finite Range Query Scheme (Fig 3.2) is well matched for attempting the mobile replica detection problem while build a random walk with two limits in such a way that every walk is determined by the experimented speed of a mobile node. The lower and upper limits will be configured to be connected with speeds less than and in overload of Vmax, correspondingly. The Energy Efficient Finite Range Query Scheme to the mobile replica detection crisis as follows. Every time a mobile sensor node travels to a novel location, every one of its neighbours' requests for a marked claim having its location and time information and determines probabilistically whether to forward the received claim to the base station. The base station calculates the speed from all two successive claims of a mobile node and achieves the Energy Efficient Finite Range Query Scheme by allowing for speed as an observed model.

Every time the mobile node's speed beats (respectively, remains below) Vmax, it should accelerate the random walk to hit or cross the upper (respectively, lower) limit and therefore guide to the base station accepting the exchange (respectively, null) suggestion in which the mobile node has been (respectively, not been) replicated. Once the base station makes a decision that a mobile node has been replicated, it eliminates the replica nodes from the network.

The Energy Efficient Finite Range Query Scheme is used for Detecting Mobile Adversary Replica Nodes in Wireless Sensor Networks. It extends replica detection scheme of probability ratio test with FRQ technique to finding the mobile replica nodes and removes the changing query ranges of mobile sensor nodes. This technique minimizes the message query transmission on data aggregation. This is verified through the experimental results. Performed simulations of the scheme under a random movement attack strategy in which the attacker lets replicas randomly move in the network and under a static placement attack strategy in which he keeps his replicas from moving to best evade detection. The results of these simulations show that the scheme quickly detects mobile replicas with a small number of location claims against either strategy.

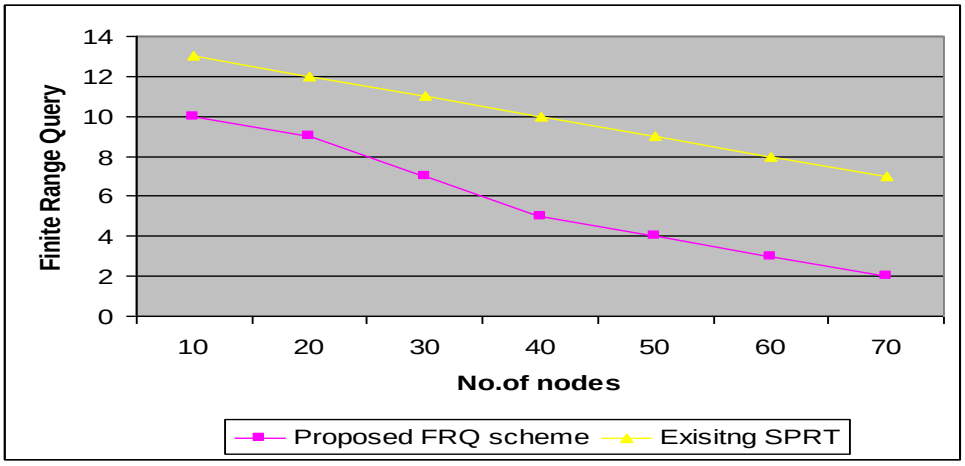

Fig 3 No. of nodes vs. Finite Range Query

The performance graph of the proposed Energy efficient FRQ scheme on Wireless Sensor Network for delay is shown in the Fig 3. Compared to an existing Sequential Probability ratio Test scheme which process and transmits the network by enhancing the query, in this, there is a great extent if more number of queries is waiting in the queue for transmission. But in the proposed FRQ, the validation scheme taken place to validate the query and it allow only the validated query to process on the network, otherwise it discarded. The finite range query is low in the proposed energy efficiency FRQ scheme in wireless Sensor Network.

IV. PROPOSED ADAPTIVE TRAFFIC DATA CONTROL WITH WIRELESS SENSOR NETWORKS

The proposed work is efficiently designed for controlling the data traffic rate occurred while eliminating the replica nodes in the wireless sensor networks. The proposed adaptive traffic data control scheme is processed under two diverse phases.

- The first phase describes the process of identifying the mobile replica nodes (acting as adversary) and eliminates the varying query ranges of mobile sensor nodes and illustrates the process of validating the range queries in the wireless sensor networks
- The next phase describes the process of controlling the traffic rate of WSN occurred while removing and validating the finite range query presents in the wireless sensor networks

The first process is to remove the replica nodes present in the wireless sensor networks. The replica detection scheme of probability ratio test with Finite Range Query (FRQ) is to detect replica node attacks in mobile sensor networks. If nodes are moving around in the network, a benevolent mobile node will be treated as a replica because of its incessant change in location. And also it describes the query validation process in continuation with an existing identification of mobile replica nodes in finite range query scheme. By validating the query in wireless sensor networks,

the mobile replica nodes are removed entirely and it reduces the loss of data occurred while making a transaction between the nodes in the network environment.

The next process describes the process of controlling the traffic data in WSN to enhance the data transmission between the sink and the base station. Numerous sources nodes require accounting data to a sink node, producing the funnelling consequence where the traffic load enhances since the distance to the sink node reduces. To control the packet generation rate at the sinks and intermediary nodes, present an adaptive traffic data control scheme. The traffic data occurring at the sink is controlled based on the flow of the original node's presence.

Consider N sensor nodes. Each node contains a definite quantity of data to be processed to a distinct bottom station. The nodes can generate data traffic, in adding to route traffic fashioned by other nodes. Consequently, every node can perform together as a source, and a router. The node models the surroundings at interrupted period, instruct the information into data packets, and drive them away to a middle base station or sink. The flow initiating from Node i be fi , and ri be the rate at which flow fi is introduced into the system. Assign the rate ri to flow fi that is both fair and efficient. Note that, ri is the rate at which node i introduces flow fi into the system, and does not contain the rate at which node i ahead traffic.

A. Eliminating replica nodes in WSN

The Finite Range Query Scheme is used in the previous work made to endeavoring the mobile duplication detection problem whereas construct an arbitrary pace with two restrictions in such a way that each pace is dogged by the research rapidity of a mobile node. The lesser and higher limits will be configured to be associated with speeds below and in the burden of Vmax, likewise. Every time a mobile sensor node schedules to a new location, each one of its neighbors desires for an obvious state having its position and timely information and decides possibility of whether to promote the received state to the base station.

The base station evaluates the speed from all two consecutive states of a mobile node and accomplishes the Energy Efficient Finite Range Query Scheme by permitting for speed as a practical model. Once the base station makes a decision that a mobile node has been replicated, it eliminates the replica nodes from the network.

B. Validating the range query of nodes in WSN

The validation of query is processed at three stages of communication in wireless sensor network environment. The first stage of query processing is made with the identification of the original node in the network environment. Even the finite range queries are used for the removal of mobile replica nodes, there is a great extent of nodes to be extracted or discarded by the attacker. In this sense, it is necessary to validate the query by identifying the node authorized id given by the certified authority. The node identification query is processed depending on node id, key value pairs.

After verifying with the nodes present in the wireless sensor network, the valid nodes are available. The node communication is based on sending and receiving the query and outcome with the free nodes for passing the message from source to destination. For sending the message, the sending query must contain a valid node id which is given by the authorized entity and the key value pairs for sharing the message with the destination.

Before delivering the message, it is necessary to check the destination node id by the query validation scheme. The query validation scheme openly communicates with every node to authenticate the packet transmission and link feature by inspecting the node id, key value pairs provided by the authorized entity. It establishes the action of every node based on its contribution in the communications. Now the network is designed with the original nodes in the network to process.

V. EXPERIMETAL EVALAUTION

Simulated the proposed adaptive traffic data control scheme in a wireless sensor network by using the NS-2 network simulator. In the simulations, set up n nodes consistently at arbitrary surrounded by a 900 × 900 square, by means of n changeable amongst 100 and 1000. Determine the mobile sensor node movement patterns. In particular, to exactly estimate the presentation of the system, use the RWM model in which each node progress to an arbitrarily selected position with an arbitrarily chosen speed among a predefined minimum and maximum speed.

Guess the standard unit disc bidirectional communication representation and change the message range, so that every node will include roughly 40 neighbors on average. The moving mobile sensor networks stays there for a predefined pause time. After the pause time, it then randomly chooses and moves to another location. This arbitrary progression is constant during the simulation period. All simulations were performed for 1,000 simulation seconds.

Fixed a pause time of 25 simulation seconds and a minimum moving speed of 1.2 m/s of each node. Each node uses IEEE 802.11 as the medium access control protocol in which the transmission range is 60 m. To emulate the speed errors caused by the inaccuracy of time synchronization and localization protocols, alter the calculated speeds with maximum speed error rate. The concert of the proposed Adaptive Traffic Data Control Scheme (ATDCS) in WSN is measured in terms of

- Energy utilization,
- Traffic control rate,
- Delay
- Reliability
- Data Loss

The Adaptive Traffic Data Control Scheme for traffic data control in wireless sensor networks that seeks to consign a fair and efficient rate to every node. The proposed ATDCS needs all nodes to observe their traffic rate, based on the dissimilarity of which every node chooses to raise or fall of the communication rates of itself and its upstream nodes. The traffic data control is invoked at every node transmitting through the gateway node, which termed as the control period. The simulations of the proposed adaptive traffic data control scheme under an arbitrary association attack strategy in which it process the packet transmission range of the network. The results indicate that the proposed data traffic control mechanism can accomplish gradually high good put, is capable to achieve fairness for all nodes in the wireless sensor networks to obtain the finest communication rates rapidly.

Data loss can occur on any device that stores data. Although any loss of data, even a simple misplacement, is by definition technically a loss, with is the permanent loss of data that is important to your business' ongoing success. Data loss occurs due to human error, hardware and file corruption

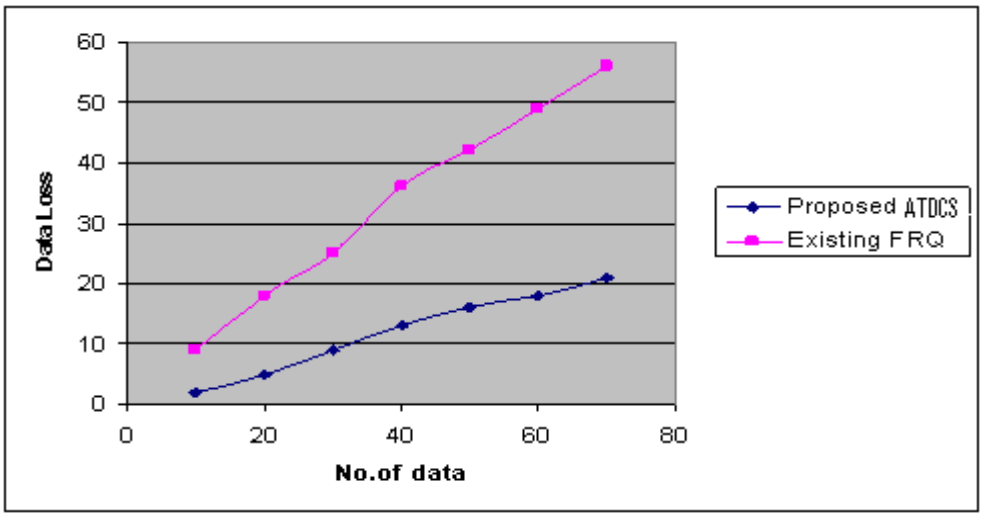

Fig.4 No. of data vs. Data loss

Fig 4 describes the data loss occurred when the amount of data increases in the wireless sensor networks. The data loss in the wireless network is high when use the finite range query scheme. If the number of query processing exceeds the limit, then the chance of losing the data from the wireless sensor network is high. To protect the data from lost, in this work used the query validation scheme to validate the query and formed the query processing more effectively.

The performance graph of the proposed ATDCS in Wireless Sensor Network for data loss is shown in the Fig 4 Compared to an existing Finite Range Query for detecting mobile replica nodes, the proposed scheme in WSN outperforms well. At last, it is being concluded that the proposed scheme in WSN efficiently validate the query based on the presence of data. The validation is performed based on the node key value pairs, node id based on its presence.

VI. CONCLUSION

Experimental assessment is carried out to evaluate the performance of the proposed framework Adaptive Traffic Control Scheme. ATDCS Framework is implemented in NS-2 simulator. A link is processed among two nodes if they are positioned inside the transmit range of every other nodes in the network. The source node and the destination node of every communication request are arbitrarily chosen. Alternate Traffic Control Scheme is used to control the data flow rate at the sink based on the original nodes presence in the wireless sensor networks.

Performance results of ATDCS is compared with the existing Sequential probability Ratio Test (SPRT) technique, by producing the 35 to 45 % better reliability, 10 to 15 % lesser energy utilization, 20 to 30 % decreased traffic control rate, and 50 to 60 % lesser delay in Adaptive Traffic Data Control Scheme.

REFERENCES

[1] Jie Jia., Chen Liu., Jian Chen., Xueli Wu., "*Design of Energy Aware Movement-Assisted Deployment in Wireless Sensor Network*," IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 2012

[2] Junyoung Heo., Jiman Hong., Yookun Cho., "*EARQ: Energy Aware Routing for Real-Time and Reliable Communication in Wireless Industrial Sensor Networks*," IEEE Transactions on Industrial Informatics, Volume: 5 , Issue: 1, 2009

[3] Jun-Zhao Sun., "*QoS Aware Query Processing Algorithm for Wireless Sensor Networks*.," Journal Of Computers, Vol: 3, No: 11, 2008.

[4] Xie Yi., Xiao Weidong., Tang Daquan., Tang Jiuyang., Tang Guoming., "*A Prediction-based Energy-conserving Approximate Storage and query processing schema in object-tracking sensor networks*," IEEE International Conference on Computer Science and Automation Engineering (CSAE), Volume: 2, 2011

[5] Yuan He., Mo Li., "*COSE: A Query-Centric Framework of Collaborative Heterogeneous Sensor Networks*," IEEE Transaction on Parallel and Distributed Systems, Vol: 23, No: 9, 2012

[6] D. Prabhakaran., D.Gowdhami., D.Suresh Babu., "*Detection of Node Replication Attacks in Mobile Sensor Networks*.," International Journal of Electronics and Computer Science Engineering, 2011

[7] S. L. Ullo., A. Vaccaro., G. Velotto., "*Performance Analysis of IEEE 802.15.4 based Sensor Networks for Smart Grids Communications*," Journal of Electrical Engineering: Theory and Application (Vol.1/Iss.3), 2010

[8] Jun-Won Ho., Wright, M., Das, S.K., "*Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis*," IEEE INFOCOM 2009

[9] Divakar M N., RajuTumkur., " *Detecting of mobile replica node attack in wireless sensor networks using sequential hypothesis testing*." International Conference on Computing and Control Engineering, ICCCE, 2012,

[10] Ram V Prabha., and P Latha., "*An Overview of Replica Node Detection in Wireless Sensor Networks*," IJCA Proceedings on International Conference in Recent trends in Computational Methods, Communication and Controls, ICON3C, 2012.

