International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

# A RELIABLE STRATEGY AGAINST POWER DISSIPATING ATTACKS IN HIERARCHICAL WIRELESS SENSOR NETWORKS

**Nida Ambreen [1], Rubeena Naz[2],E. Channaveeramma[3]**

*[1,2]M. Tech Student, DCN, Navodaya Institute of Technology, Raichur-584103*
*[3]Asst Prof. Dept .of ECE, DCN Navodaya Institute of Technology, Raichur-584103*

---

**Abstract -** *Efficient energy and reliability are critical concerns in wireless sensor network (WSN) design. In this work we are aimed to develop an energy-efficient reliable strategy against power dissipate attacks, especially the denial-of-sleep attacks, which can reduce the lifetime of WSNs rapidly. The well-known reliable process usually awake the sensor nodes before these nodes are allowed to perform the security processes. Therefore, the practical method is to simplify the authenticating process in order to cut down the energy consumption of sensor nodes and increase the performance of the MAC protocol in countering the power dissipate attacks. The scrutiny shows that the proposed strategies can counter the replay attack and forge attack in an energy-efficient way.*

***Key Words*: MAC protocol, Cluster, sensor nodes, wireless sensor network .**

## 1. INTRODUCTION

Large-scale sensor networks are deployed in numerous application domains, and the information that we collect are used in decision making for critical frameworks. Information's are rushed from multiple sources through transitional processing nodes that accumulate information. A malicious attacker may introduce additional nodes in the network or compromise existing ones. Therefore, persuade high data trustworthiness is crucial for correct decision-making.

Data provenance serves as key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging demands, such as low energy and bandwidth consumption, efficient storage and reliable transmission.

We propose a lightweight strategy to reliable transmit provenance for sensor data. The proposed approach relies on in-packet Bloom filters to encode provenance. We introduce efficient system for provenance verification and reconstruction at the base station [8]. In addition, we enhance the reliable provenance strategy with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed approach both analytically and empirically, and the results prove the capability and efficiency of the lightweight reliable provenance strategy in identifying packet forgery and loss attacks.

## 2. OVERVIEW OF RELIABLE STRATEGY AGAINSTPOWER DISSIPATION ATTACKS

Low Energy consumption and enhancing the lifetime of WSNs is the major concern in today's world, the duty cycle based protocol is one of the major strategies in energy conservation of WSNs. This duty-cycle based WSN MAC protocols, sensor nodes are transposed from awake/active to sleep state periodically and these nodes move into sleep mode after little idle period.

B-MAC is the Low Power Listening (LPL) based WSN MAC protocol. In this technique receiver wakes up periodically to sense the preamble from the source and then to receive and process the data. When the source requires to send data, it sends a long preamble to cover the sleep period. The LPL based MAC protocol is an asynchronous protocol, decouples the source and receiver with time synchronization [lo].This long preamble design of LPL based protocol consumes the major energy of both source and receiver. Based on the variant initiator, this duty-cycle strategy will be classified into two types: sender-initiated strategy and receiver initiated (RI) strategy. For purpose, the X-MAC protocol is one of the sender-initiated strategies to improve B-MAC protocol by replacing the long preamble with short preambles, which allows the receiver to send acknowledgment (ACK) back to the sender as soon as it senses the preamble.

The RI-MAC protocol is one of the receiver-started strategies to lowers the channel occupancy time of a pair of a source and receiver, allows the sender to send data to the receiver as soon as it senses the beacon. However, current layer-2 protocol plans are inadequate to protect a WSN from Denial-of-Sleep attack. The energy conservation is one of the major goals of WSN plan, whereas the reliable strategy always consumes more energy of model. There is no well decision rule to compromise the needs between energy conservation and reliable strategy.

The Denial-of-Sleep is one of the power exhausting attacks of WSNs. An anti-node can send fake data packets to sensor node of unprotected WSNs to initiate unnecessary transmissions repeatedly [12]. Without reliable technique, an anti-node can broadcast a fake preamble frequently in the source-initiated strategies. Though the receiver cannot tell

real preamble and the fake one, the receiver will receive and process the information from the anti-node. This attack will preserve the receiver is as long as the data transmission sustains, which exhausts the battery of nodes rapidly. Moreover, an anti-node can replay a fake preamble ACK to the sender. Thus, the sender will start to send the data to the anti-node but it will never receive the right data ACK. Similarly, the sender may send data repeatedly and exhausts the battery of node rapidly.

In receiver-initiated strategies, an anti-node can broadcast a "fake beacon" to cheat sender to process and send the data to the anti-node but it will never receive the right data ACK. An anti-node can send a "fake beacon ACK" to the receiver.

Thus, the receiver will start to receive and process the data from the anti-node. If attack packets interval is shorter than the sleep period of a Network, then communication with neighboring nodes in a WSN could be impede by attack packets. Consequently, no packets from the attacked nodes can be delivered, which issues with a jamming-like scenario. However, unlike the physical jamming attack, no consecutive signals or packets are required for the packet attack. A well-planned periodical attack, packet can be applied to perform like jamming-like attack, which may lowers the performance of a duty-cycle strategy for WSN operating and achieve energy conservation of an anti-node during the adversaries. As a result, the source and receiver required mutual authentication strategies to counter attack. In conventional wireless reliable technique, with symmetric key or asymmetric, encryption algorithm is used to send the data.

The wireless sensor networks prefer the symmetric algorithm to avoid the complicated computing and heavy energy consumption. But the encrypted message makes the battery exhaustion even worse under Denial-of- Sleep attack. The anti-node can send the encrypted "garbage" data to receiver. This attack forces the receiver to decrypt the data. Before the receiver identifies that the data is "garbage", the receiver consumes more power to receive and decrypt data. These processes also preserve sensor nodes to stay awake for longer period [14].

Accordingly, an easy and fast mutual authentication strategy is required to populate with MAC protocol to counter the Denial-of-Sleep attack. In any adopted reliable technique of WSNs, the sensor nodes need to be waked before collecting data and authenticating reliable properties.

The practical method is to simplify the reliable process when detorriate the power exhausting attacks.

The Plan of reliable strategies in above layers may be coupled with the fixed data link layer technique.

Here, a cross-layer plan of reliable strategy populating the MAC protocol, Two-Tier Energy-Efficient Reliable Strategy ($TE_2S$), is proposed to protect the WSNs from the above attacks based on our preliminary frameworks.

This cross-layer design involves coupling two layers at plan time without creating new interface for information exchanging at runtime.

The principles and features of the proposed reliable strategies are:

- Energy conservation
- Low complexity
- Mutual authentication
- Symmetric encryption
- Dynamic session key created with challenge text
- Capability to counter the Denial-of-Sleep attack
- Integrating the MAC protocol

This strategy implies with the hash-chain to create the dynamic session key, which can be used for mutual authentication and the same encryption key.

The only computations of dynamic session key are the hash functions, like MD5 or SHA-l, these are very simple and fast. By accommodating with MAC protocol, there is no extra packet compared with the prevailed MAC plans. The two-tier plan can investigate and impede with the attacks at various check points. The combination of low complexity reliable process and multiple check points design can protect against attacks and send the sensor nodes back to sleep mode as soon as possible.

The reliable analysis shows that these strategies can counter the replay attack and forge attack, and the energy analysis shows that this strategy is energy efficient as well. The detailed energy distribution of energy analysis also shows a new possible decision rule to compromise the needs between energy conservation and reliable strategy.

### 2.1 Data Flow Diagram

A **data-flow diagram** (**DFD**) is a graphical representation of the "flow" of data through an information system. This type of flow diagrams can mostly be used for the visualization of data processing (structured design). The data items in this type of flow diagram flow from either external data source or an internal data store to an internal data store or an external data sink

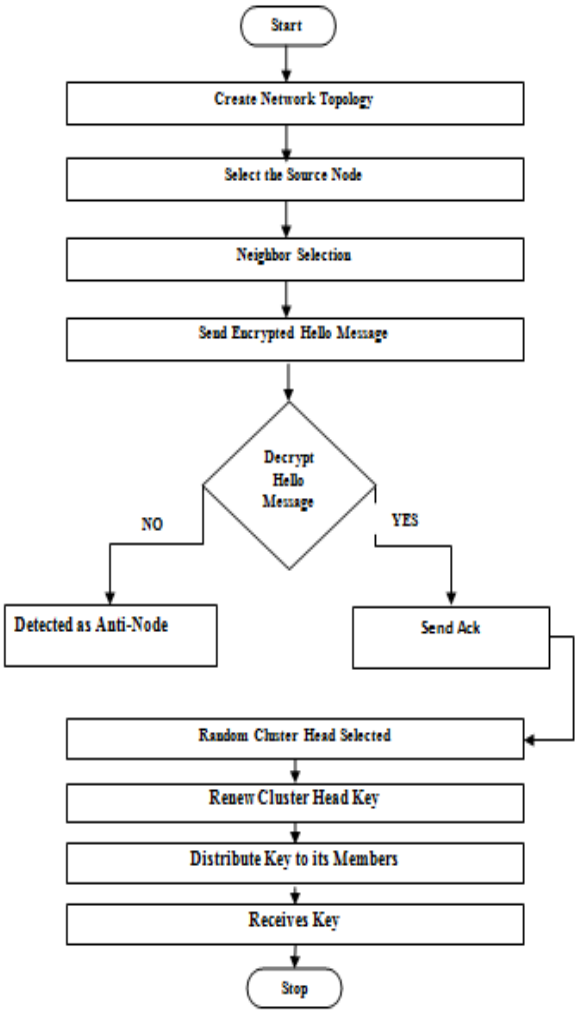


**Fig-1:** Data Flow Diagram

### 2.2 System Flow Diagram

1. The Flow chart is also called as bubble chart. It is a simple graphical formalism that can be used to present a model in basis of input data to the system, various processing carried out on this data, and the output data is moderated by this system.

2. The data flow structure is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that collaborates with the system and the information flows in the system.

3. Flow diagram shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical method that narrates information flow and the transformations that are applied as data moves from input to output.

4. A Flow diagram may be used to constitute a system at any level of abstraction. This may be partitioned into levels that constitutes growing information flow and functional detail.

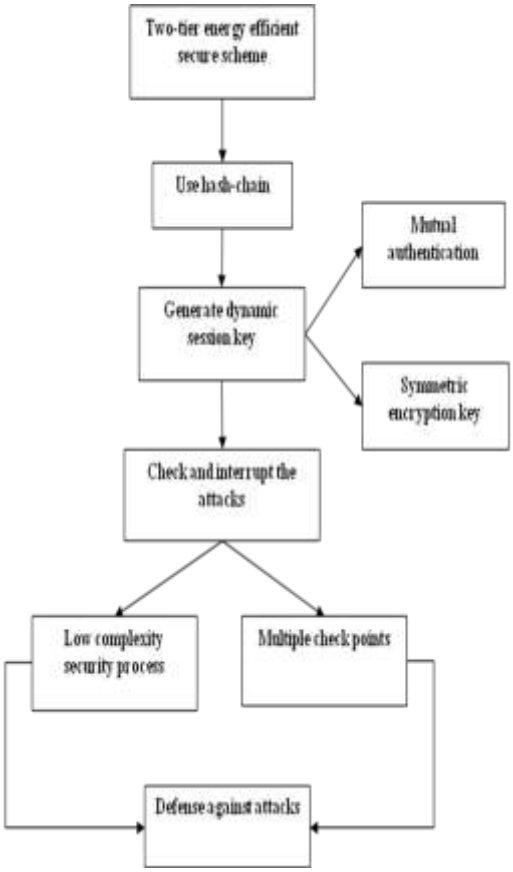


**Fig -2**: System Flow Diagram

## 3. PROPOSED SYSTEM

### 3.1 Modules Description

#### 3.1.1 Topology Creation

In this project we are employing wireless sensor network. In this network, the nodes are static and attached. The sensor nodes are recognizing the information and then send to the server. If the source node sends the packet, it will send through the in-between nodes. The nodes are communicates only within the communication range. So, we have to find the node's communication range [26].

#### 3.1.2 Anti-Node Detection

In order to make the network robust against adversaries, an authenticated broadcasting technique, such as the $\mu$ TESLA in SPINS may be required in this stage. In the authenticated broadcasting technique, with the help of the pre-shared key a plaintext "*Hi*" message is encrypted.

If the sensor cannot decrypt the message received successfully, the source is indicated to be as anti-node. Thus, the normal nodes and the anti-nodes can be distinguished. Therefore, we built the network topology without anti-nodes in order to make the network safe. Notice that an external attack can be intercepted by the operation of stage I. Here in this work, we do not have a lightweight countermeasure to protect against authenticated malicious nodes. If the authenticated node is compromised and performs malicious activities, a strategy for expelling the compromised nodes is required.

### 3.1.3 Cluster Formation

Each sensor updates a random waiting timer, broadcasts its localizes via a "*Hello*" signal, and listens for its neighbor's "*Hello*." The sensors that hear many neighbors are good candidates for starting new clusters; those with least neighbors should choose to wait. Sensors set their neighbor information and cut down the waiting random time based on each new "*Hi*" message received. This encourages those sensors with all neighbors to become cluster heads.

If a neighbor declares itself to be a cluster head, the sensor cancels its own timer and joins the neighbor's new cluster. After applying the ADTCA, there are three separate kinds of sensors: (1) the cluster heads (2) sensors with a naming cluster ID (3) sensors without naming ID of a cluster, which will join any nearby cluster and become 2-hop sensors. This topology of the ad-hoc network is constituted by a hierarchical collection of clusters.

### 3.1.4 Gateway Selection

To interconnect two adjacent non-overlapping clusters, one cluster member from each cluster must become a gateway. According to the process of cluster formation, sensors can obtain local information and know the number of neighboring sensors in adjacent clusters.

Therefore, given the local information, sensors may initialize their counters for gateway selection. Based on the counter, cluster heads broadcast messages to trigger the gateway selection process.

After applying the procedure for dictate the gateways, the gateway nodes broadcast messages to update the connectivity information and activate the linked cluster construction.

### 3.1.5 Key Distribution

In this domain, two symmetric are considered to be as shared keys, gateway key, and a cluster key which are encrypted by the pre-spread key and these are spread locally. A cluster key is a key distributed by a cluster head and all its cluster members, which is mainly used for securing locally broadcast messages, e.g., routing control information, or securing sensor messages. Moreover, in order to form a secure communication channel between the gateways of adjacent clusters, a symmetric exchanged key is used to encrypt the sending message. Another challenge encrypted by a cluster key or a gateway key may be made to protect against anti-nodes that have not been found out. Therefore, the reliability of intra-cluster communication and inter-cluster communication are established upon a cluster key and a shared gateway key, respectively [19].

### 3.1.6 Key Renewal

With the same encryption key for extended periods may occur a cryptanalysis risk. To protect the sensor network and prevent the attackers from getting the keys, key renewing may be obligatory. Initially all cluster heads (CHs) choose an originator to start the "key renewals", and then it will send the list to all cluster heads in the network. After selecting the originator, it initializes the "Key renewal" process and sends the lists to its neighboring clusters by gateways. Then the cluster head restores the two keys from the key pool and distributes the two new keys to their cluster members locally.

### 3.1.7 Performance Evaluation

In this section, we evaluate the performance of simulation. We are getting the x-graph for evaluate the performance. We choose the some evaluation metrics: Packet delivery ratio – the ratio of the total number of packets received by the destination node to the number of packet sent by the source, End-to-End delay – the time taken to be data sent from source node to destination node. And calculate the Energy consumption by the sensor node. Along these evaluation metrics we have to evaluate the simulation performance in x-graph.

## 3.2 Design

### 3.2.1 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be attained by moitoring the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system.

The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding other steps and preserving the process simple. The input is designed in such a way so that it provides reliability and ease of use with preserve the privacy. Input Design considered the following things:

- Some data should be given as input

- The data should be arranged or coded
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

### 3.2.2 Design Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This plan is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is attained by generating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry will be effortless and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is inputted it will check for its validity. Data can be entered with the help of screens. Appropriate information are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

### 3.2.3 Output Design

A quality output is one, which meets the needs of the end user and gives the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output plan it is regulate how the information is to be displaced for instant need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Planning computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is sketch so that people will find the network which can use easily and effectively. When analysis design computer output, they should Identify the specific output that is required to meet the needs.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections.
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

### 3.3 Sequence Diagram

A sequence structure flow is a kind of interaction, that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

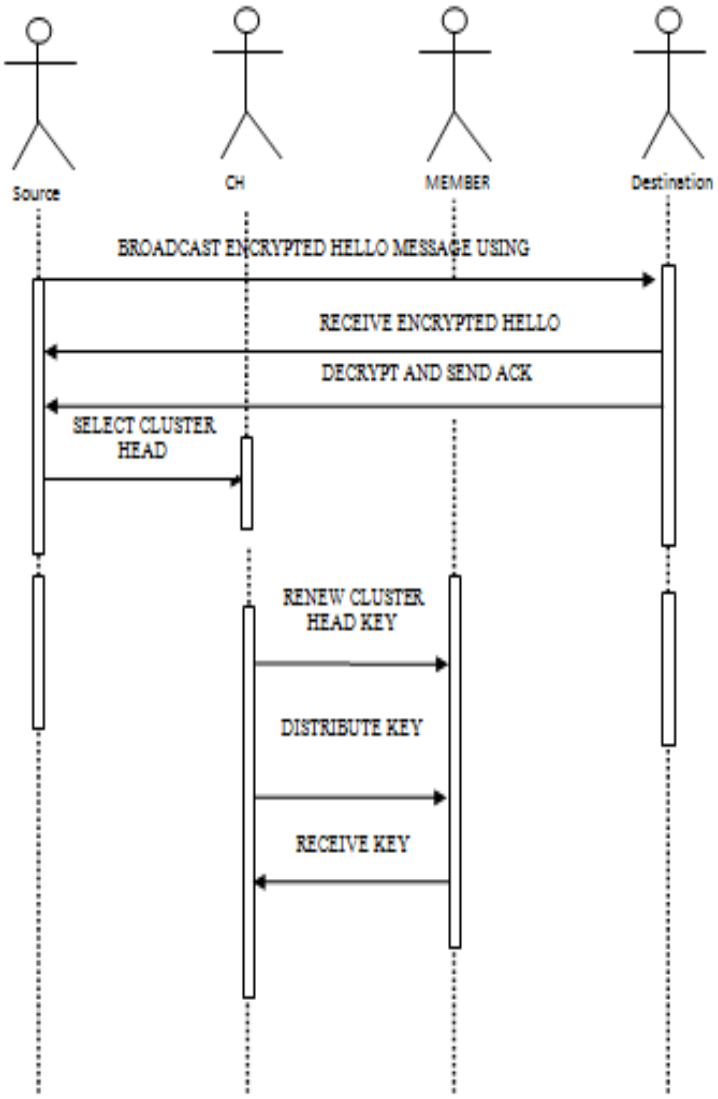


**Fig-3:** Sequence Diagram

### 3.4 Activity Diagram

Activity structures are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. Activity flow can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

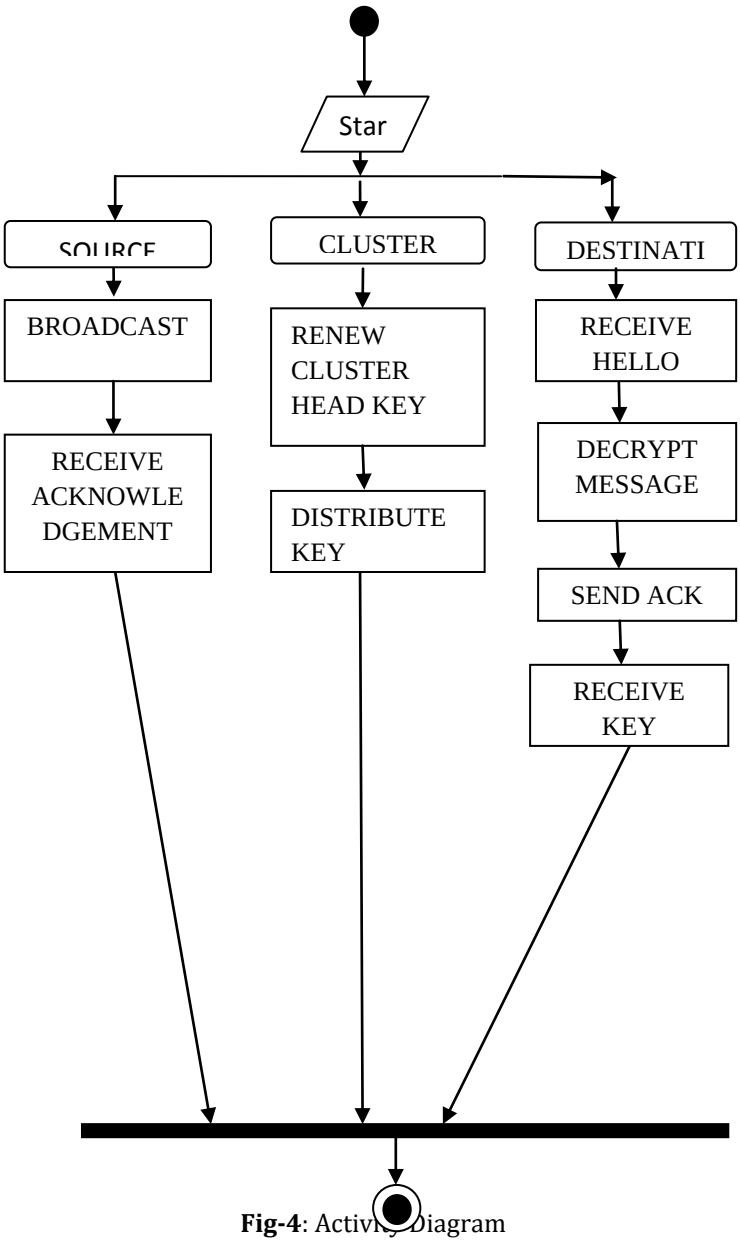


**Fig-4**: Activity Diagram

## 4 Performance Evaluations

### 4.l Delay Graph

Shows graph of delay versus speed as speed increases delay increases. At decreasing speed delay seems constant

**Fig-5:** Delay Graph Comparison between Existing and Proposed Scheme

### 4.2Energy Consumption

Graph of energy versus time in mile second. As time increases energy decreases. At start energy is considered to be 1ooJ. Packet drop ratio is 1o packets per mile second

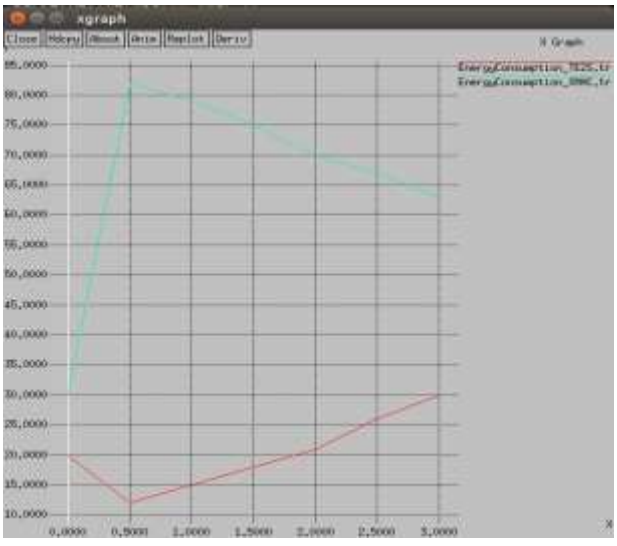

**Fig- 6:** Energy Consumption Graph compared between Existing and Proposed Scheme

### 4.3 Packet Delivery Ratio

Graph of Packet Delivery ratio describes no. of packet received to the no. of packet sent measured in %.

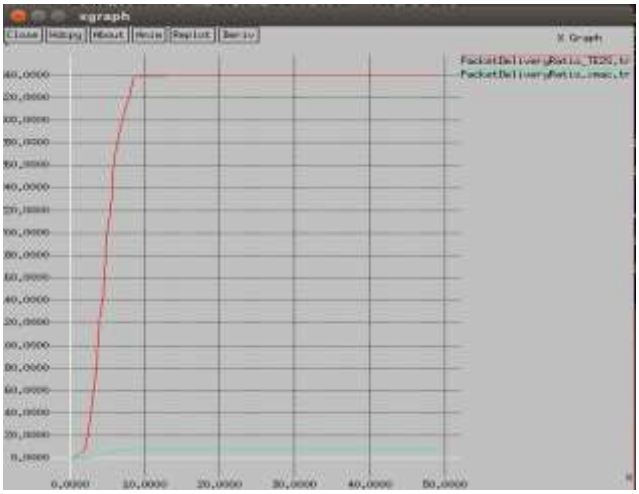

**Fig-7:** Packet Delivery Ratio Graph compared between Existing and Proposed Scheme

4.4 Throughput

Throughput Graph describes no. of packet sent in particular time measured in kb/s.

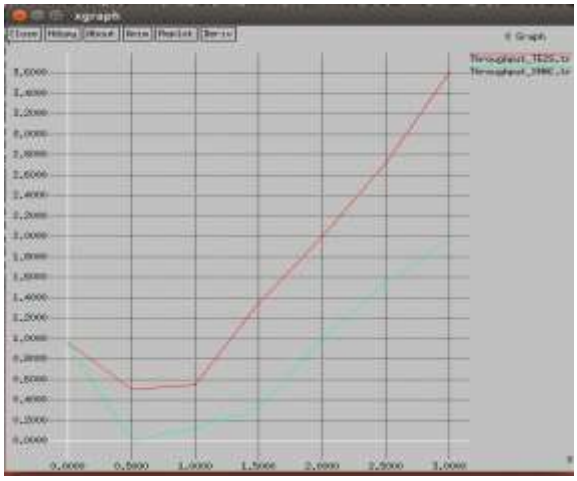

**Fig-8:** Throughput Graph compared between Existing and Proposed Scheme

## CONCLUSION

We proposed a cross-layer design of energy-efficient reliable strategy populating the MAC protocol. Extra packet is not involved in the original MAC protocol method. This strategy can cut down the authenticating process as short as possible to mitigate the effect of the power dissipating attacks. By combination of low complexity security process and multiple check points, the proposed method can protect against attacks and send the sensor nodes back to sleep mode as soon as possible. The security analysis shows that this strategy can counter the replay attack and forge attack. The energy analysis identifies the operating mode precisely, including the MCU and radio modules. The simulation results of normalized energy consumption for normal condition, which has no attacks, shows that the proposed scheme increases up to 6o% more efficient than that of the X-MAC protocol in energy consumption. The simulation results of normalized energy consumption for attack conditions also shows that the proposed strategy can save times of energy consumptions than X-MAC or RI-MAC does, which also can enlarge the lifetime of WSNs under attacks. The energy analysis shows that this strategy is efficient in both sender-initiated plan and receiver-initiated plan. The overall results show that the proposed method $TE_2S$ strategy can attain the same throughput performance with less energy consumption. Moreover energy consumption of the proposed strategy under various duty cycles can be checked to provide more extensive simulation results to support the efficiency of $TE_2S$ strategy in the later state. The detailed analysis of energy distributions clears up the proportions of energy consumptions for each state of MCU and radio modules. This analysis shows that the MCU consumes only a slit portion on entire energy consumption. Thus, applying a well design of light-weight reliable strategy to increase the MCU loading but to cut down the energy consumption of radio module is a reasonable decision rule of coordination between energy conservation and security needs in design of WSN applications.

## REFERENCES

[1] G. Halkes, van Dam T, and Langendoen K. G., “Comparing energy saving MAC protocols for wireless sensor networks,” Mobile Netw. Appl., vol. l0, n0. 5, pp. 783–79l, 2O05.

[2] A. Bachir, M. Dohler, K. K. Leung, and T. Watteyne, “MAC essentials for wireless sensor networks,” IEEE Commun. Surv. Tuts., vol. 12, no. 2, pp. 222–248, Second Quarter 2O1O.

[3] J. Kabara and Calle M, “MAC protocols used by wireless sensor networks and a general method of performance evaluation,” Int. J. Distrib. Sensor Netw., vol. 2O12, pp. 1–l1, 2O12, Art. ID 834784.

[4] M. Li, A. V. Vasilakos and Z. Li, “A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues,” Proc. IEEE, vol. lO1, no. l2, pp. 2538–2557, Dec. 2O13.

[5] R. Carrano, Passos.D , L. C. S. Magalhaes, and C. V. Albuquerque, “Survey and taxonomy of duty cycling mechanisms in wireless sensor networks,” IEEE Commun. Surv. Tuts., vol. 16, no. l pp. 181–194, First Quarter 2O14.

[6] P. Huang, L. Xiao, S. Soltani, N. Xi , and M.W. Mutka, “The evolution of MAC protocols in wireless sensor networks: A

survey," IEEE Commun. Surv. Tuts., vol. 15, no. l, pp. 1O1–12O, First Quarter 2O13.

[7] W. Ye, D. Estrin, and J. Heidemann, "An energy-efficient MAC protocol for wireless sensor networks," in Proc. 21st Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), Los Angeles, CA, USA, 2OO2, vol. 3, pp. 1567–1576.

[8] Van Dam T and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in Proc. 1st Intrnl. Conf. Embedded Network. Sensor Syst. (SeuSys), Los Angeles, CA, USA, 2OO3, pp. 17l–18O.

[9] J. Polastre, J. Hi1l, and D. Cu1ler, "Versatile low power media access for wireless sensor networks," in Proc. 2nd Intrnl. Conf. Embedded Network. Sensor Syst. (SeuSys), Baltimore, MD, USA, 2OO4, pp. 95–1O7.

[10] M. Buettner, R. Han, E. Anderson, and G. V. Yee, "X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks," in Proc. 4th Intrnl. Conf. Embedded Network. Sensor System. (SenSys), Boulder, Co, USA, 2OO6, pp. 3O7–32O.