A SECURE PATH SELECTION METHOD FOR HIGHLY SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

N. Divya & Dr. R. Muralidharan

Ph.D Research Scholar, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore.

Head, Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore.

Abstract: WSN is a conveyed arranges presented to an open situation, which is helpless against malevolent nodes. To discover malevolent nodes among a WSN with mass sensor nodes, this paper presents a vindictive recognition technique dependent on essential and optional way arrangement. A Sensor is a gadget that reacts and identifies some kind of contribution from both the physical or ecological conditions, for example, pressure, heat, light, and so on. Uses of remote sensor systems incorporate home automation, road lighting, military, medicinal services and modern procedure checking. As remote sensor systems are circulated across enormous geological region, these are helpless against different security dangers. This influences the presentation of the remote sensor systems. The effect of security issues will turn out to be progressively basic if the system is utilized for strategic applications like strategic front line. All things considered, arrangement situations, the likelihood of disappointment of nodes is more. Advanced ROSE, a novel strength upgrading calculation for scalefree WSNs, is proposed with different key age calculation. Because of asset imperatives in the sensor nodes, conventional strategies which include enormous overhead calculation and correspondence are not plausible in WSNs. The outcomes shows that the situation with numerous center node (CN) with non-covering network requires less time for malignant node location with better accuracy when contrasted with the situation with single Center Node with framework.

Keywords: Center node, Malicious Node detection, Path Selection, Multiple Key Generation

I. INTRODUCTION

Wireless sensor organize (WSN) is comprised of a gathering of sensor nodes that cooperate in a gathering other to complete an allotted task (for example environmental factors management, target development, and so on.) at that point educates the accumulated information through a wireless medium to a base station or sink node [5].

A WSN is an assortment of low force and ease gadgets that are known as sensor nodes (SN). These SN are extremely little in size and their capacity utilization and computational force is likewise less. Sensors, microcontrollers, memory gadget, power source, receiving wire are totally coordinated in one SN [4].

This significant component additionally once in a while comes as risky issue during the information transmission, supposing that the malicious nodes is available in the system, this nodes happens an unsettling influence to whole directing procedure [3].

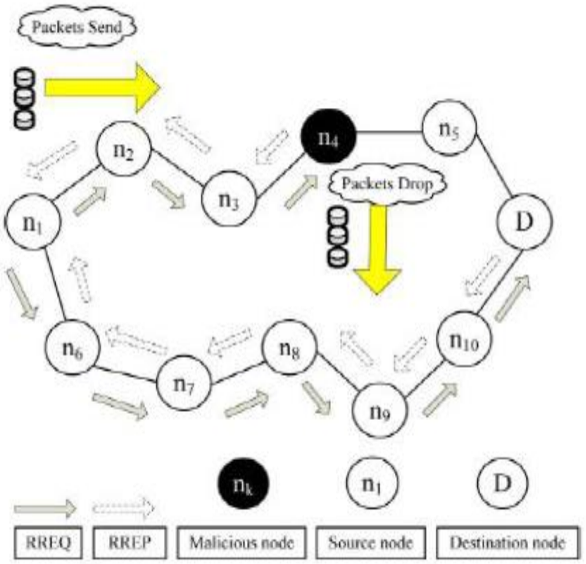


Figure 1: Packet dropping by malicious node n4

In the above figure 1, shows how the malicious nodes are draw in information parcels in the system by fashioned course reaction. By this bogus RREP the malicious nodes convey the chose information parcels to other un-characterized goal or bogus goal.

Because of attributes of sensors and WSN, Providing Quality of Service (QoS) is particularly basic and as yet testing issue in information correspondence among the sensors, sink nodes and base stations [1].

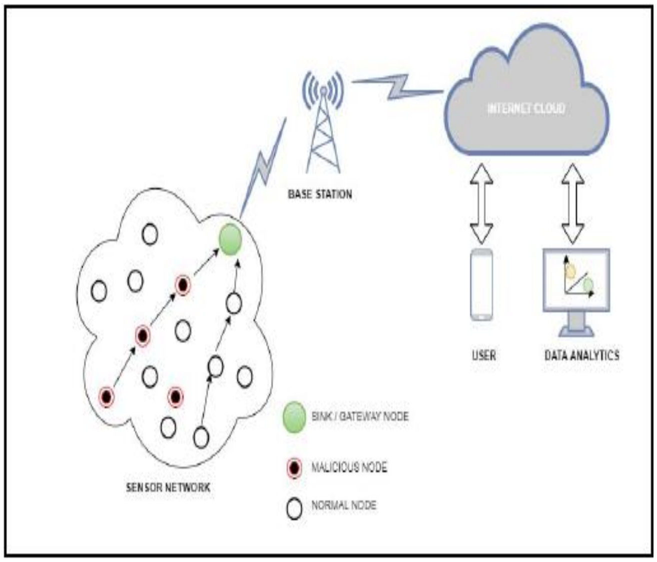


Figure 2: Malicious Activities in WSN – Generic Architecture

The sink node has progressively computational force nearly too every single other node and has extraordinary effect on lifetime of WSN. A portion of the malicious nodes may refuse any assistance, could adjust the information and transmits to sink node as appeared in figure 2.

As of late, the idea of trust and notoriety has been broadly used to create security plans for WSNs. Trust is characterized as the certainty and confidence of a node in the capacity, consistency, and dependability of different nodes, which can be resolved dependent on immediate or backhanded perception of the nodes' practices. A trust decided dependent on direct perception is called direct trust, while that decided dependent on different nodes perceptions and conclusions is called circuitous trust or notoriety [10].

The remainder of this paper is organized as follows. Area II surveys probably the latest research on trust assurance and malicious node discovery and confinement in WSNs. The proposed method is clarified in Section III. The reenactment condition, results and conversations are portrayed in Section IV. At last, Section V presents investigate ends and calls attention to certain suggestions for future innovative work.

II. BACKGROUND STUDY

Devaraju, B. M., et al. [1] Cross Layer and Management Plane Integration Approach for recognition and counteraction of malicious exercises in WSN has been introduced in this paper. This methodology has the benefits of decreasing the preparing postponement and correspondence delay by dodging malicious exercises in WSNs.

Dai, H., et al. [2] proposed a multivariate characterization based malicious node discovery calculation for WSN to utilize a little piece of type-realized nodes to identify malicious nodes among the other sort obscure nodes. We extricated 4 properties of sensor nodes in a WSN and demonstrated the WSN to a quantifiable element vector space. In this space, all the named tests are found out through the multivariate grouping based location calculation.

Kumar, S., et al. [5] As to improve the system lifetime just as for solid and proficient correspondence in wireless sensor arrange the convention utilized ought to be vitality productive, which can be additionally accomplished by utilizing a decent quality grouping procedure. In this paper, PSO based strategy for malicious node discovery and picking a bunch head in wireless sensor arrange is proposed. The calculation proposed depends on the three information parameters, for example remaining vitality of the node, supported inclusion and the connection quality, which chooses the capability of every single node in the WSN.

Singh, S. S., et al. [6] counteraction of node disappointment is finished utilizing AODV directing convention, Check Point Recovery calculation and Network Topology Management. These three techniques are consolidated together to locate the best course for parcel transmission absent a lot of vitality misfortune and to identify the node whose vitality level is going to deplete utilizing a Static node which close the Dynamic node about the vitality drop in a specific node. The Dynamic node looks for the closest node whose vitality level is high and furthermore has less number of connections.

Shivaji, S. S., et al. [8] energy efficient intrusion detection system (EEIDS) approach is proposed and actualized. In EEIDS, Bayesian methodology is utilized for expectation of sensor nodes vitality utilization. Bayesian methodology use priori data of sensor nodes and probability capacity to figure the back estimation of nodes, so it gives preferred vitality expectation over markov chain model. Expectation procedure not burns through more effort to screen the nodes to distinguish malicious node.

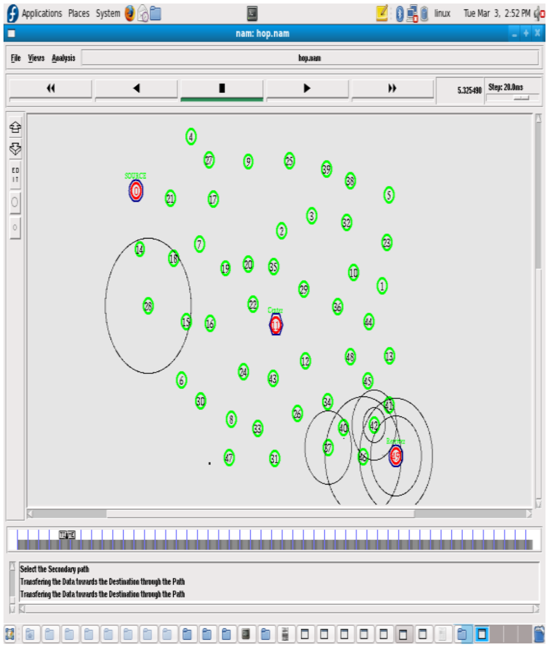
III. SYSTEM MODEL

Since the rise of WSN in 1996, numerous calculations have been introduced for the malicious node discovery. In [3], a particular based technique is proposed to quickly exam whether an action of a node observes the directing convention leads by utilizing agreeable screen nodes in the system.

Emerged is intended to be handled in a brought together framework. Before ROSE works, every node sends its own directions and neighbor rundown to the unified framework through the multihop framework. After we accomplish the streamlining results as indicated by ROSE, the brought together framework sends the new neighbor rundown to every node through the multi-jump framework.

A) Independent Edges

Every one of nodes I, j, k, and l must be in the correspondence scope of the other three nodes. This guarantees each node can build up an association with others.



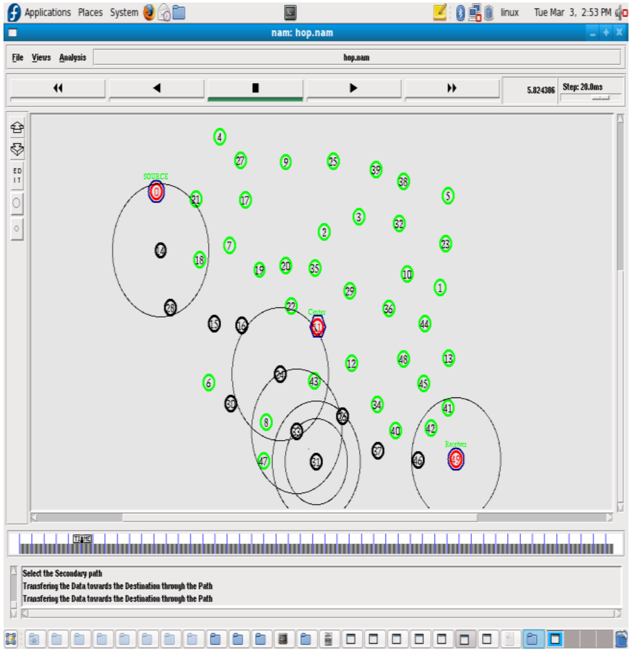
Select the Secondary path
Transferring the Data towards the Destination through the Path
Transferring the Data towards the Destination through the Path

Figure 3: Node Initialization

In figure 3 represents the node initialization for Node 0 to 49. The source node considered as 0. And 49th node considered as Destination. The Node 11 has been considered as the center Node (CN).

B) Degree Difference Operation

All the neighbors of a high degree node have high degrees. At the point when the node comes up short, its neighbors can supplant its unique capacity and guarantee the availability of the remaining system. Consequently, the obliteration of malicious assaults is debilitated, all things considered, in WSNs.



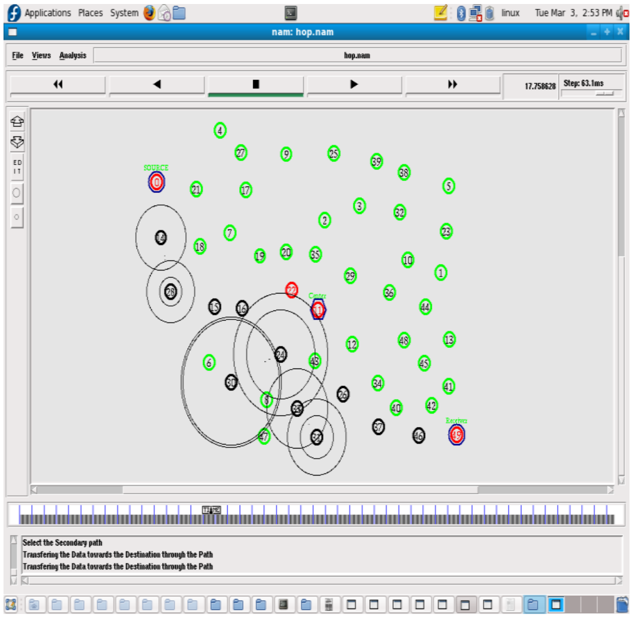
Select the Secondary path
Transferring the Data towards the Destination through the Path
Transferring the Data towards the Destination through the Path

Figure 4: Primary Path selection

In figure 4 represents the primary path selection for the source to destination.

c) Angle Sum Operation

Notwithstanding the trademark that nodes in a ring have comparative degrees, another attribute of the onion-like structure is that in each ring of nodes there exists a huge number of edges generally even concerning the center of the system. As needs, we present an edge entirety activity here that acquires the onion-like structure by misusing this trademark. As far as we could possibly know, we are the first to abuse this trademark.



Select the Secondary path
Transferring the Data towards the Destination through the Path
Transferring the Data towards the Destination through the Path

Figure 5: Malicious Node activity in primary path

In figure 5 shows the data flow over the primary path and finding the malicious node activity.

Algorithm 1 Scale-free network topology modeling in WSNs

```
Input: $N$, $V$ , $r$, $m$
Output: $Lst_i$
procedure BANETWORKBUILD($A$)
 for all $v_i \in V$ do
    $v_i \leftarrow$ receiveStartingSignal()
     Setting timer
     if Timer of $v_i$ expired then
broadcastStartPacket($v_i$)
$v_i \leftarrow$ receiveDisconnectNeighborDegree()
if the degree of nodes in $V_i$ are all zero then
            $\Pi\ Local\ (j)=1/N_i$
else
  for all $v_j \in V_i$ do
   $\Pi\ Local(j)=d_j/\sum_{i=1}^{n} d$
 end for
         end if
         use Roulette method select $m$ nodes in $V_i$ base on $\Pi$ $Local(j)$
           $Lst_i$= Modify neighbor list of $v_i$
        broadcastEndPacket($Lst_i$)
       broadcastStartingSignal()
end if
end for
end procedure
```

In algorithm 1 depicts First, a recently *i* joined node *i* gets a beginning sign and sets a clock (Lines 3 and 4). At the point when the clock terminates, it sends an add association solicitation to all neighbors. At that point, it gets the degree data of nodes that are in the nearby universe of node *i* (Lines 6 and 7). Next, node *i* computes the association likelihood of each neighbor dependent on input data. In the event that the level of each neighbor node is zero, node I interface with them with equivalent likelihood (Lines 8 to 9); in any case, node *i* figure the association likelihood as indicated by the level of neighbor nodes (Lines 11 to 12). The codes in Lines 15 to 16 depict the way toward building up m edges between node *i* and its neighbors by the roulette technique. Next, the neighbor list Lsti is refreshed and communicated to all neighbor nodes. At long last, node I communicates a beginning sign for the unjoined nodes (Line 18).

```
Algorithm 2 Degree difference operation
Input: $A, E, N, r$
Output: A
 procedure DEGREEDIFFERENCEOPERATION($A$)
   for all edges in E do
     Randomly select $e_{ij}$ and $e_{kl}$
     if $e_{ij}$ and $e_{kl}$ are unmarked && $e_{ij}$ and $e_{kl}$ are a pair of independent edges then
       A←A'
       if Networkfullyconnected() and R(A) ≥ R(A) then
          A←A
     End if
   End if
Mark this pair of edges ($e_{ij}$ and $e_{kl}$).
End for
End procedure.
```

Algorithm 2 depicts the procedure of the degree distinction activity, which is executed after the displaying of the scale free system topology in WSNs.

```
Algorithm 3 Angle sum operation
Input: $A, E, N, r$
Output: A
procedure ANGLESUMOPERATION($A$)
 for all edges in $E$ do
  Randomly select $e_{ij}$ and $e_{kl}$
   if $e_{ij}$ and $e_{kl}$ are unmarked && $e_{ij}$ and $e_{kl}$ are a pair of independent edges then
     $A_1$←A (Remove $e_{ij}$ and $e_{kl}$ in A and Add $e_{il}$ and $e_{jk}$ to $A_1$)
       $A_2$←A (Remove $e_{ij}$ and $e_{kl}$ in A and Add $e_{ik}$ and $e_{jl}$ to $A_2$)
      SUM=max($SUM_A$, $SUM_{A1}$, $SUM_{A2}$)
         If Network Full connected() and R($A_1$)≥ R(A) and SUM == $SUM_{A1}$ then
           A←$A_1$
           Else if Network Full connected() and R($A_2$)≥ R(A) and SUM == $SUM_{A2}$ then
             A←$A_2$
       end if
       end if
   Mark this pair of edges($e_{ij}$ and $e_{kl}$)
     end for
   end procedure
```

Algorithm 3 portrays the procedure of the point aggregate activity, which is executed after the degree distinction activity. The factors utilized in the algorithm are as per the following.

- A_1, A_2: the nearness network after a trade activity dependent on the total of encompassing edges.

A couple of autonomous edges is haphazardly chosen, e_{ij} and e_{kl} (Lines 2 to 3). At that point, the entirety of the encompassing plots for all the three association strategies is determined.

The association strategy with the most extreme point total is chosen (Lines 5 to 7). In the event that it is the underlying association strategy, the trading activity is skipped and the following round of choosing edges starts; in any case, the contiguousness framework A to A1 or A2 is modified dependent on the estimation of SUM. On the off chance that the modification keeps the system topology associated and doesn't lessen the estimation of R, it is acknowledged (Lines 8 to 12). Something else, the modified nearness framework is come back to An and the algorithm starts the following round of choosing edges.

Algorithm 4: Multi-key Generation:

ACK requires all affirmation parcels to be carefully marked before they are conveyed and checked until they are acknowledged. In any case, we completely comprehend the additional assets that are required with the presentation of advanced mark in WSNs. To address this worry, we actualized the two plans. The objective is to locate the most ideal answer for utilizing advanced mark in WSNs. Uneven key cryptography defeats the key administration issue by utilizing distinctive encryption and unscrambling multiple key sets. Knowing about multiple key, say the encryption key, isn't adequate enough to decide the other key - the unscrambling key. Subsequently, the encryption key can be made open, gave the decoding key is held uniquely by the gathering wishing to get scrambled messages (thus the name open/private key cryptography). Anybody can not utilize the open key for other people, open keys and to encode a message, just for beneficiary can unscramble it.

The scientific connection between people in general/private key pair allows a general principle: any message encoded with one key for one space of the pair can be effectively decoded uniquely with that key's partner. To encode with the open key methods you can decode just with the private key for space by opening. The opposite is additionally valid - to scramble with the private key methods you can decode just with the open key.

ACK requires all insistence packages to be painstakingly set apart before they are passed on and checked until they are recognized. Regardless, we totally fathom the extra resources that are required with the introduction of advanced imprint in WSNs. To address this concern, we realized the two plans. The goal is to find the best response for using advanced imprint in WSNs. Lopsided key cryptography crushes the key organization issue by using unmistakable encryption and unscrambling various key sets. Thinking about different key, say the encryption key, isn't sufficiently satisfactory to choose the other key - the unscrambling key. In this manner, the encryption key can be made open, gave the unraveling key is held remarkably by the social affair wishing to get mixed messages (along these lines the name open/private key cryptography). Anyone can not use the open key for others, open keys and to encode a message, only for recipient can unscramble it.

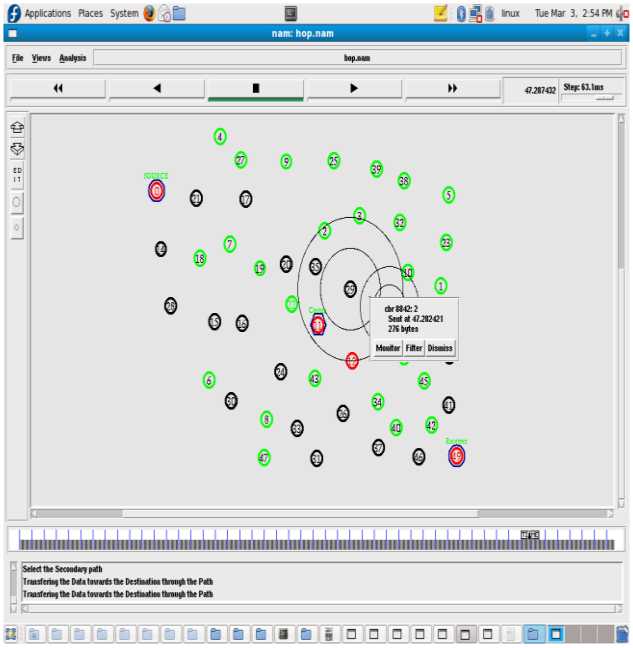
The logical association between individuals as a rule/private key pair permits a general standard: any message encoded with one key for one space of the pair can be successfully decoded exceptionally with that key's accomplice. To encode with the open key strategies you can unravel just with the private key for space by opening. The inverse is furthermore legitimate - to scramble with the private key techniques you can disentangle just with the open key.

Encryption process:

- **Set the number**
- **Set sham image**
- **Combine symbol table and dummy symbol table to symbol table with dummy (STWD)**
- **Set turned byte and pivot image table with sham**
- **Transpose the image table after revolution**
- **Shift the image table after transposition**
- **Complement the image table after move**
- **Packed control byte table**
- **Shift the control byte table**
- **Combine image table after**
- **complement and control byte after move to**
- **get Cipher Text (CT)**

Decryption process:

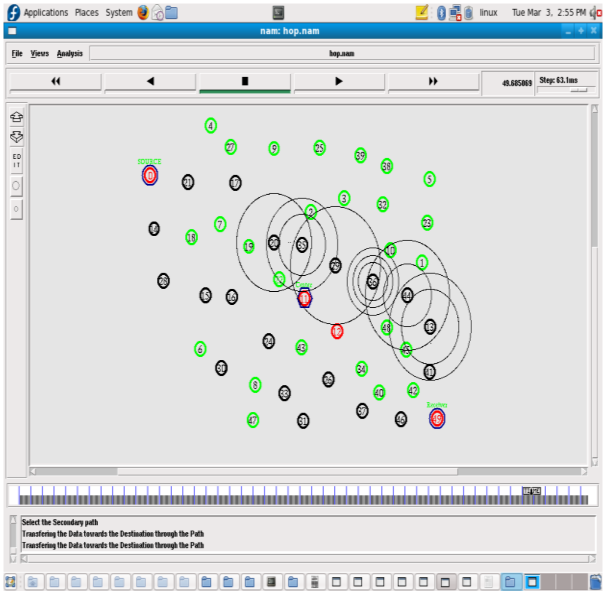
- **Get CT**
- **Separate cipher text into control byte after separation (CBAS) and symbol table after separation (STAS)**
- **Shift control byte after detachment**
- **Pack control byte after move**
- **Complement image table after detachment**
- **Shift image table after supplement**
- **Transpose the image table after move**
- **Rotate image table after transposition**
- **Get plaintext (PT).**



Select the Secondary path
Transfering the Data towards the Destination through the Path
Transfering the Data towards the Destination through the Path

Figure 6: Secondary path selection.

In Figure 6 represents the secondary path selection in source 0 to destination 49.



Select the Secondary path
Transfering the Data towards the Destination through the Path
Transfering the Data towards the Destination through the Path

Figure 7: Data flow over the secondary path

In figure 7 shows the data flows to the secondary path and avoiding the malicious activity node.

The degree distinction and edge entirety tasks improve the vigor of sans scale systems differently. We included the limitation that just if the estimation of R increments would this is able to trade be acknowledged. Along these lines, the request for the two tasks has no negative consequences for the whole without scale organize. So as to accomplish better heartiness improvement impacts, we tried the presentation when the two activities were consolidated in various requests. In view of the recreation results, AROSE executes the degree distinction activity first and the edge entirety activity second. The mix of the degree contrast and the edge total tasks renders the structure of the sans scale arrange topology exceptionally near being onion-like. In the interim, the two tasks maintain a strategic distance from the estimation of R to the best degree conceivable. Along these lines, the calculation productivity of AROSE is exceptionally high.

IV. DISCUSSION

In the wake of running the tcl contents with NS2, we get the follow records. At that point, we use gape to dissect the follow documents for extricating highlight vector of every node. The reproduction results are Energy correlation, delay, PDR, correspondence cost. The details of comparison have been exhibits as the Figure 8-12.

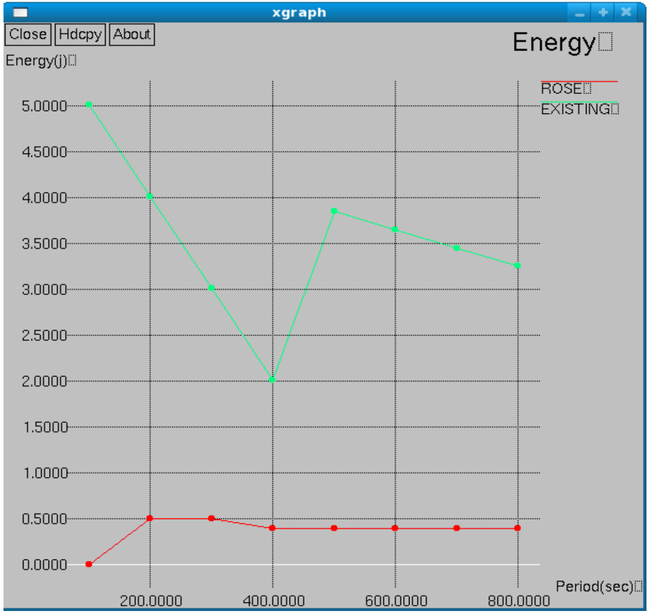


Figure 8: Energy Comparison

In figure 8 shows the energy comparison of the existing and proposed system. In x axis denotes the period in seconds. And y axis denotes the energy.

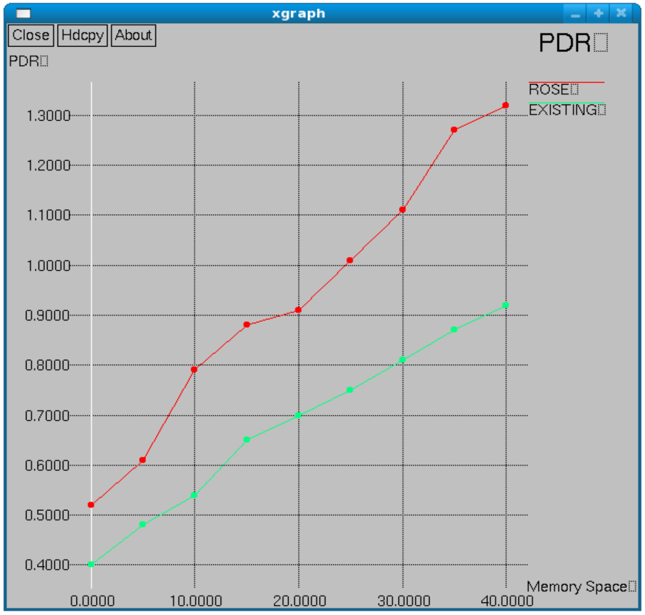


Figure 9: Comparison chart for Pact delivery ratio

In figure 9 compares the pact delivery ratio. In x axis denotes the Memory Space and y axis denotes the PDR.

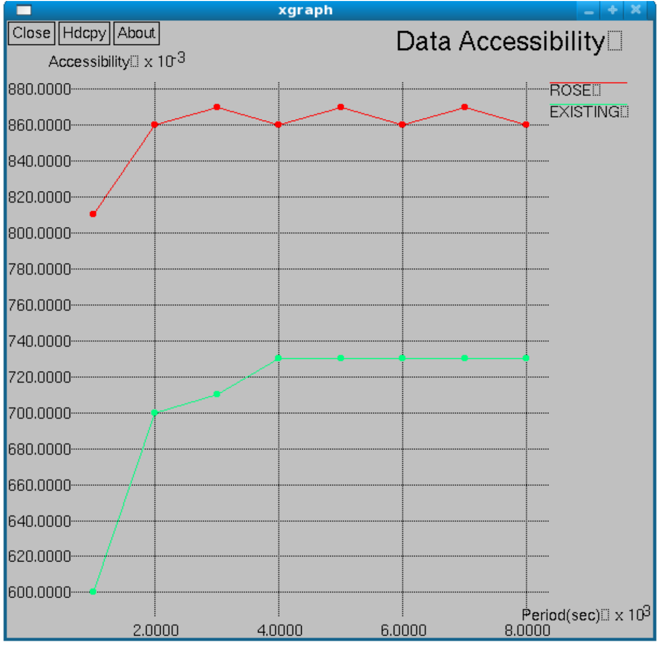


Figure 10: Data accessibility chart

In figure 10 compares the Data accessibility in existing and proposed system. In x axis denotes the period in seconds. Y axis denotes the Accessibility in 10^3

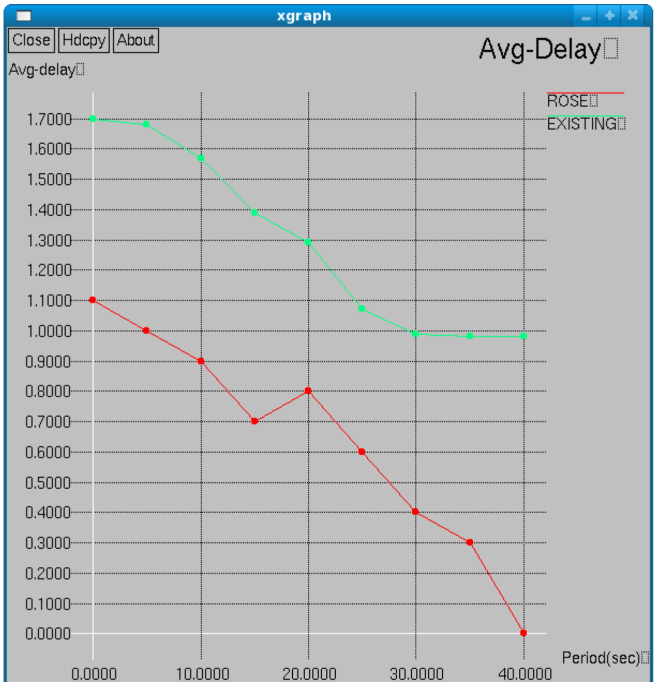


Figure 11: Average Delay comparison

In figure 11 shows the delay comparison in existing and proposed system. In x axis denotes the period in seconds. And y axis denotes the average delay.

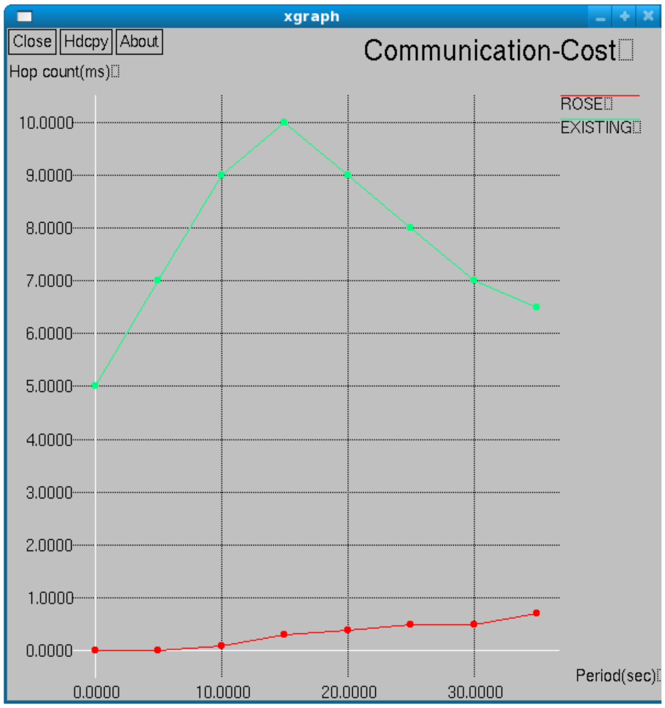


Figure 12: Communication chart comparison.

In figure 12 shows the existing and proposed communication cost. In x axis denotes the period in seconds. Y axis denotes Hop count.

Problem Statement

A without scale topology, ROSE endeavors the position and degree data of nodes to adjust the edges to look like an onion-like structure, which has been demonstrated to be strong against malicious assaults. In the interim, AROSE keeps the level of every node in the topology unaltered to such an extent that the subsequent topology remains without scale. The broad trials results confirm that our new displaying procedure without a doubt produces sans scale organize topologies for WSNs, and ROSE can fundamentally improve the heartiness of the system topologies created by our demonstrating methodology. Emerged comprises of two stages: the degree contrast and the edge aggregate activity. The two tasks are expected to change the system topology toward the onion-like structure. The mix of a degree contrast activity and a point total activity in the algorithm makes sans scale arrange topologies quickly approach an onion-like structure without changing the first force law appropriation. At last, the presentation of AROSE was assessed on sans scale arrange topologies having various sizes and edge densities. The reenactment results show that ROSE fundamentally improves vigor against malicious assaults and holds the first sans scale property in WSNs simultaneously. ROSE needs the data of the whole sans scale arrange topology to help the choice of free edges. Accordingly, the procedure for upgrading power against malicious assaults can't legitimately be run in a disseminated framework. ROSE necessitates that worldwide data be gathered into the unified estimation. Altogether high system thickness negatively affects the exhibition or effectiveness of AROSE. Subsequently, when the system thickness is controlled inside a reasonable range, this upgrading procedure can accomplish better outcomes and its finishing requires a shorter time.

V. CONCLUSION

In this paper, we proposed a ROSE with multi key age based malicious node location algorithm for WSN to utilize a little piece of type-realized nodes to identify malicious nodes among the other kind obscure nodes. A recently proposed algorithm called AROSE with Multi key Generation was intended for improving the power of without scale systems against malicious assaults. The blend of a degree contrast activity and a point entirety activity in the algorithm makes sans scale arrange topologies quickly approach an onion-like structure without changing the first force law conveyance. At last, the exhibition of AROSE was assessed on without scale arrange topologies having various sizes and edge densities. The recreation results show that ROSE altogether improves heartiness against malicious assaults and holds the first without scale property in WSNs simultaneously. To improve high accuracy rate recognition for future work.

VI. REFERENCES

[1] Devaraju, B. M., & Raju, G. T. (2018). Cross Layer and Management Plane Integration Approach for Detection and Prevention of Malicious Activities in WSN. 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT).

[2] Dai, H., Liu, H., Jia, Z., & Chen, T. (2012). A Multivariate Classification Algorithm for Malicious Node Detection in Large-Scale WSNs. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[3] Guruprasanna, & Sujatha, M. R. (2016). A novel approach to avoid malicious attack to enhance network in WSN. 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT).

[4] Jaint, B., Indu, S., Pandey, N., & Pahwa, K. (2019). Malicious Node Detection in Wireless Sensor Networks Using Support Vector Machine. 2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE).

[5] Kumar, S., & Mehfuz, S. (2019). A PSO Based Malicious Node Detection and Energy Efficient Clustering in Wireless Sensor Network. 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN).

[6] Singh, S. S., & Bevish Jinila, Y. (2016). Sensor node failure detection using check point recovery algorithm. 2016 International Conference on Recent Trends in Information Technology (ICRTIT).

[7] Wang, W., Xu, J., & Wang, J. (2009). Detection and location of malicious nodes based on source coding and

multi-path transmission in WSN. 2009 11th IEEE International Conference on High Performance Computing and Communications.

[8] Shivaji, S. S., & Patil, A. B. (2015). Energy Efficient Intrusion Detection Scheme Based on Bayesian Energy Prediction in WSN. 2015 Fifth International Conference on Advances in Computing and Communications (ICACC).

[9] Vinayagam, S. S., & Parthasarathy, V. (2014). IPTTA: Leveraging Token-based node IP assignment and verification for WSN. 2014 International Conference on Science Engineering and Management Research (ICSEMR).

[10] Zawaideh, F., Salamah, M., & Al-Bahadili, H. (2017). A fair trust-based malicious node detection and isolation scheme for WSNs. 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS).