JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

THE REGULATOR NODE TECHNIQUE FOR SELECTIVE NODE ATTACK PREVENTION IN RANDOM WIRELESS SENSOR NODE NETWORK

[1]Gurbir Kaur, [2]Harmandeep kaur, [3]Dr Supreet Kaur

[1]Student, [2]Student, [3]Professor
[1]Khalsa of Engineering and Technology, Amritsar,Punjab, India

Abstract : WSN may split due to a number of reasons, including early deployment, battery drain, or hardware issues (WSNs). As a result, the majority of the sensors lose communication utilising the sink connector, disrupting the data delivery process. One potential approach is to populate impart nodes to unite the barriers and restore communication. The same device is applied is used by the invasion exposure programme in a standardized WSN to find unusual movement attackers or unauthorised incursions in a field of interest. A thorough analysis performed prior to the deployment can adequately assess the quality of deterministic detector node disposition. The suggested method is used to move nodes around in order to discover faked nodes. The proposed method uses less energy than the old one, which is an enhancement.

IndexTerms **- WSN, RN, K-mean, Energy Consumption**

I. Introduction

In recent ages, the arena of WSN has built-up speedily. This article briefly introduces WSN and their uses in the fields of environment, structure monitoring, industrial applications, health, military, vehicle detection, crowding regulator and RFID tags. With the growth of the RSSF, low-cost sensors with wireless communication capabilities that can perceive various types of environmental conditions and data processing become available. There are diverse sorts of routing etiquettes, reliant on the use and network manner. The routing practice delivers network paths rssf is found in various uses such as civilian and military around the world covering enemy invasion exposure object. [1]

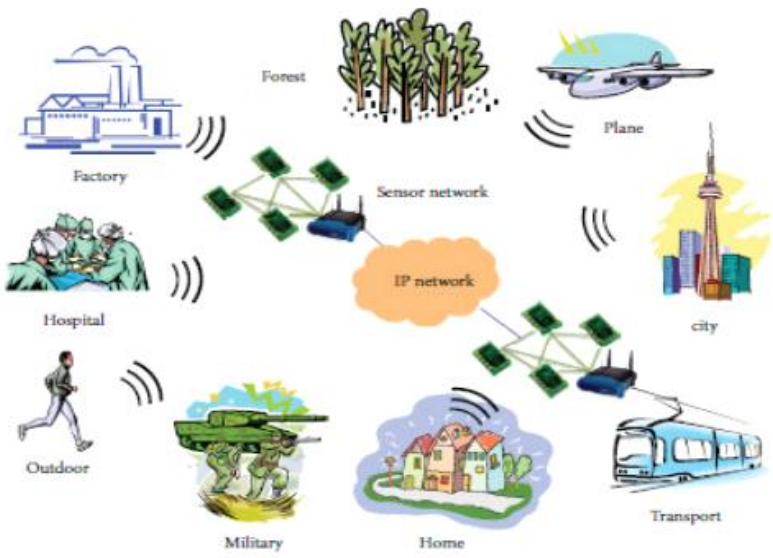


Fig1 Wireless sensor Network. [2]

1 WIRELESS SENOR NETWORK APPLICATIONS

The WSN is utilized in various applications nowadays. The "WSN " network plays vital role in military and several industries like health, and Environmental. WSNs are broadly positioned in the medical area. These networks, generally mentioned to WSN medical network, are now cutting through key parts of the healthcare industry and are able to improve the eminence of patient care without dropping comfort. [3]

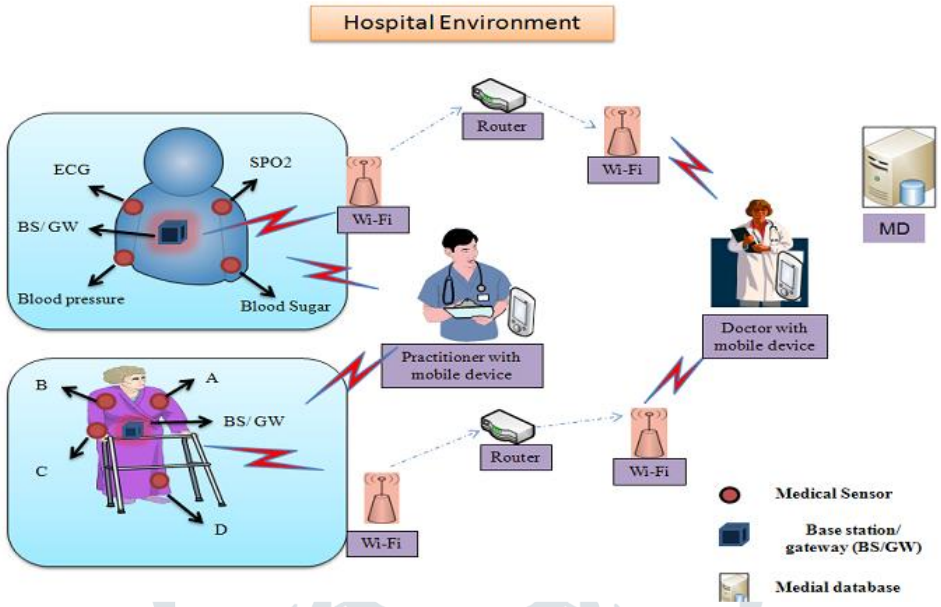


Fig2 WSN [3]

The latest development of WSN, in the guiding medium, we know that magnetic fields are steered by a firm standards, such as copper wire, coaxial cable or optical fiber. Similarly, an uncertain medium will involve the atmosphere , please do not drive. This spread routine is called wireless transmission. [4]

The Node positioning is separated into twofold in WSN: static disposition and flexible rollout. Classification criteria mainly depend on the entire sensor network It needs to be operated or the sensor devices need to be adjusted while connecting the sensor devices. Based In the Deployment Manner and Compatibility Unit[5]

1. FIXED DEPLOYMENT: Fixed Disposition picks the best location according to the optimization strategy. The place of nodes detectors held steady throughout the lifespan of the WSNS. Fixed deployments include continuous deployments and continuous deployments.

2. RANDOM DEPLOYMENT: Dynamic deployment mainly involves the positioning of robots. full presentation performance, SNS should automatically go to the precise place, then start working .[6] Random deployment is an economic deployment Method, but full coverage is not guaranteed. in order to Get the ideal coverage effect, a lot of nonsense We have to deploy. That is the way to go Applicable when the coverage requirements are not strict. However, But in some regions where rollout is problematict [7]

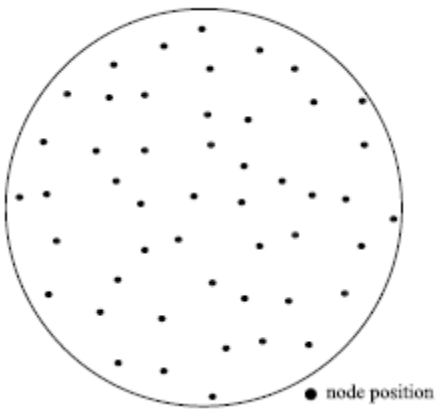


Fig 3 Node Deployment in WSN. [6]

Unlike traditional networks, WSN is lacking an independent communication infrastructure. Respectively node actions as an endpoint for detection or processing at the alike interval, and also act as a router for transmitting data packets between other nodes. In a proportion of those scenarios, putting a fresh node is necessary to place it within the broadcast spectrum of another node that is already allied to the network, which simplifies the establishment of WSN, but carries new problems and disadvantages. Using other nodes to route data packets increases the risk of network partitioning. In a arbitrary architecture, if any node stops working for some reason (battery consumption, hardware failure, etc.), the channel of conversation across active nodes get disconnected Typically, in

WSN, there is a special collector node that can work Act as a bridge to transfer data and commands between Nodes and processing centers. Lose exchange with some people. [7]

II. Related work

The WSN is form of a huge volume of small battery-powered WSN, so energy resources are imperfect. The entire network must minimize energy depletion to allow uncontrolled and unsupervised operation for extended periods of time. The basic method to diminish energy lessening and extend service life is to place sensor nodes in the network area reasonably. This effort recommends a node implantation strategy to recover the service life. Generally, using the fact that more energy is consumed from nodes near the radiator, more nodes deployed to the radiator. [8]The enhancement in technology has endorsed the progression of less value sensor nodes with readily available hardware. A WSN (RSSF) is is a dispersed self-contained system. collection of such detector nodes with limited resources. These nodes join to execute a collective aim. These detector nodes are composed of of affordable technology components that are limited in terms of battery life, memory size, and computing power. WSN are commonly installed in severe situations that are difficult to access or even full of dangers to execute various observing jobs. [9]The arbitrary positioning sensor can monitor a space with two dimensions for restrictive applications, while letting mathematical regulator of the coverage excellence it lets. In addition, centred on this pattern, useful technologies for detecting and repairing sensor faults are added to deliver system healthiness. In particular, considering the implant parameters, a mathematical formula was developed to express the chance of complete coverage when environmental characteristics change. In addition, a method is proposed to adapt the solution to the needs of various monitoring applications based on RSSF. Simulations were also performed to show the proficiency of the developed strategy, highlight some of its characteristics and evaluate its impression on the service life of the monitoring system being served[10] Intrusion detection applications on similar WSNs are distinct as a method for sensing unauthorized intrusions or abnormally moving intruders in areas of interest. The implantation quality of detector nodes can be fully determined through rough exploration before implantation. However, when random implants are required, determining the quality of implants becomes a challenge. it may involve multiple nodes to monitor each option in the detection area. This limit is called the coverage ratio k, where k is the total of nodes. The implantation quality of sensor nodes directly depends on the density and detection range of the nodes. Mainly need to implant random sensor nodes. The problem efforts on the system coverage. How do we ensure that all point in the detection area is covered by the necessary number of detector nodes, and what conditions can ensure network coverage[11] The WSN system with lowest setup and highest reach link expense, and least energy depletion is to arrange the perfect amount of detector nodes through an effective planning mechanism. Appropriate preparation will provide you with an economical deployment because it has an ideal location for sensor nodes. The positioning arrangement of detector nodes is essential to adapt to the balance nearby detector nodes can not only provide more coverage but also consume less energy. reduce energy consumption, but also cause the network coverage to become smaller.[12] Because of WSN wide use in military and civilian fields, WSN have field, but because it uses wireless means for communication, it is exposed to security attacks. There are many kinds of attacks on WSNs, such as the black hole' attacks using selective forwarding. the errant node turns like a regular node and selectively discards data packets. The assortment of one-time nodes can be arbitrary. Detecting this nature of occurrence is very tough, sometimes impossible.[13]WSNs will become a popular technology in the coming time due to its wide application in military and civilian fields. These networks vulnerable to security attacks because they are autonomous and unprotected. Some inherent functions make it impossible for sensor networks to use traditional security solutions, which require complex calculations and large-capacity memory. Many attacks on these networks can be parted into routing attacks and data traffic attacks. Some data attacks on sensors will attack the selective forwarding of nodes. Black hole outbreak, the infected node will reject all packets it forwards.[14]The article was talking about network privacy and encryption, in addition to a selective attack and a forward attack, when considering system authentication. Although utmost of the work is devoted towards attacks by contamination, in which the attacker modifies the intermediate package, only a few works is selective Data forwarding attacks or acknowledgement packets (ACK); the latter is necessary when encoding the network. [15] The WSNs consists of detection areas, base stations, the Internet, and users who can measure and predict temperature, sound, fluctuation, vibration, pressure, etc. Since data transmission is involved in RSSF and network management Protocol/Internet Protocol (TCP/IP), utilized to send data to the base station. The security of data transmission is of dominant significance because data contains valuable information. The attacker can attack any layer of the TCP/IP protocol. Network layer may be subject to selective packet drop attacks, Sybil attacks, “black hole attacks" and "denial of service attacks" (DOS). these attacks may occur can be overcome using key management procedures. Communication between nodes can only be done through these keys.[16] It is very challenging to design a WSN (RSSF) that can reliably work to discard internal packaging in the presence of an attacker. Although current trust mechanisms and preventative strategies are effective, they have several drawbacks. The prevention method transfers multiple copies of the software package to prevent intruders and cause high overhead. In a reliable mechanism, each sensor monitors its neighbors, evaluates its reliability, classifies it as reliable or unreliable and then castoffs the unreliable sensor.

Still, malicious within the system are spurious participants both the network and know exactly what stakeout nodes are. They can attacks thoughtfully to avoid being covered and castoff through the network.[17]

III. PROBLEM IN Existing System

1 In the previous system, the dispersion at random of nodes was used, and the influence of the nodes and the transmission range (usually k value) were considered in network transmission. But after making fail. Placing (activating) new nodes by expanding the radio and moving the remaining active nodes is the main method to restore connectivity in WSN. Joining nodes to a field with a

constant area can increase communication linkages amongst nodes, which may result in a higher k value, the radio transmission range is increased, allowing nodes to converse openly. This leads to problems with notice of incursions and numerous aspects of security.

2 If some wrong information can be flooded in network by malicious nodes, it will cause problems. These mean nodes can reduce network routine by triggering security attacks. Among the possible attacks, selecting a node is the furthermost critical attack that can be caused The nodes behave the same as common nodes in most cases, but will selectively discard sensitive data, data packets that report the drive of opposing forces. This selective disposal is hard to portend

3 Unauthorized nodes will stop forwarding information and randomly discard it, but will behave mean and send their own message to other vertices

4 Unauthorized nodes delaying message flow to mislead routing data across nodes is another kind of attack.

IV. PROPOSED METHODOLOGY

A navigation table (RN table), which includes details about each node, is formed by the suggested technique.

The intermediate node in the route is identified between source and location. The intermediate node's information is compared with the Regulator node RN table during the communication in the middle of nodes. Considering the comparison's implications, it decides whether it is a selective Node or a normal node. The following procedures are taken by the system model to prevent a particular node from joining the network. the network g is made up of n nodes in step 1

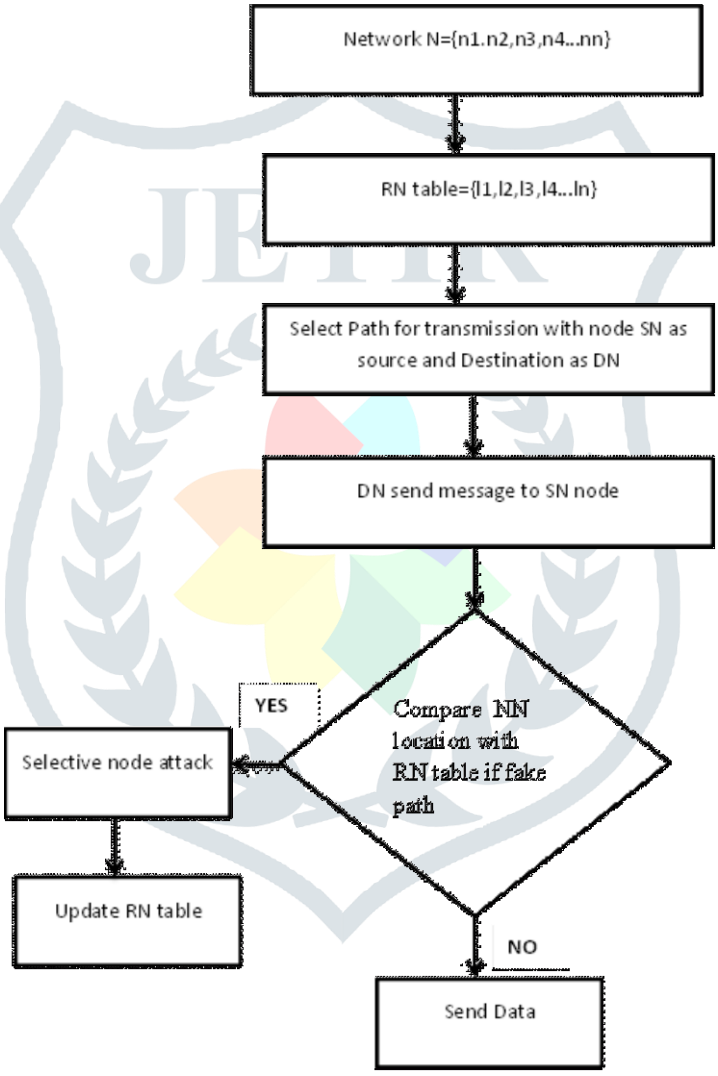


Fig 4 Flowchart

The system model goes through the following steps:

Step 1: N number of randomly placed nodes makes up the network G.

Step 2: Generate table with location li of adjacent node in transmission path to base station

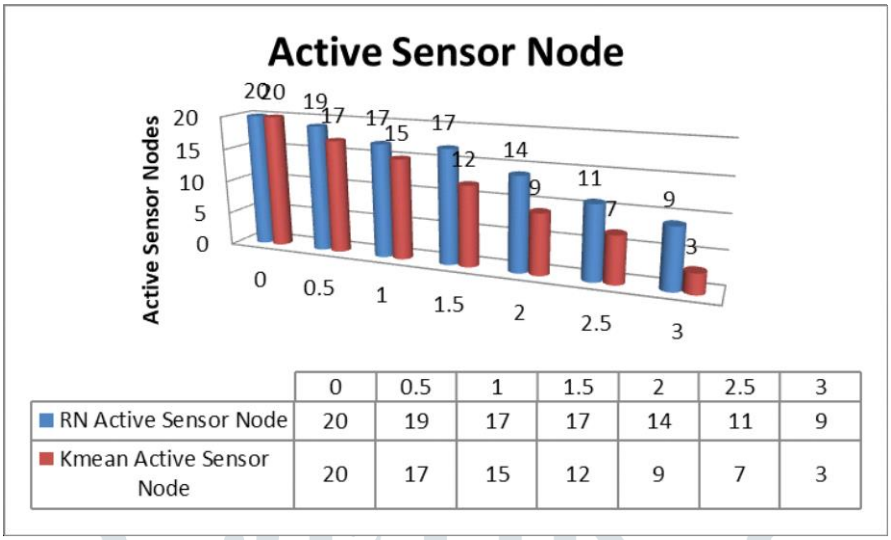
Step 3: Discover the route among the elected nodes S, D are source and destination nodes.

Step 4: Check the route and verify the Selective node activity then pass the data. While sending message the neighbor node will send location of receiving node path to base station then if any node try to send fake path it will Cut off that node and direct records after checking neighboring node table for sending path The location of nodes will broadcast by every node and after confirmation

on hello message the information will be forwarded throughout the network These nodes will be regarded as regulator nodes, and nodes alongside the trail within the region will inform the information table passed by RN.

V. Result and discussion

1 Remaining Active Sensor Nodes

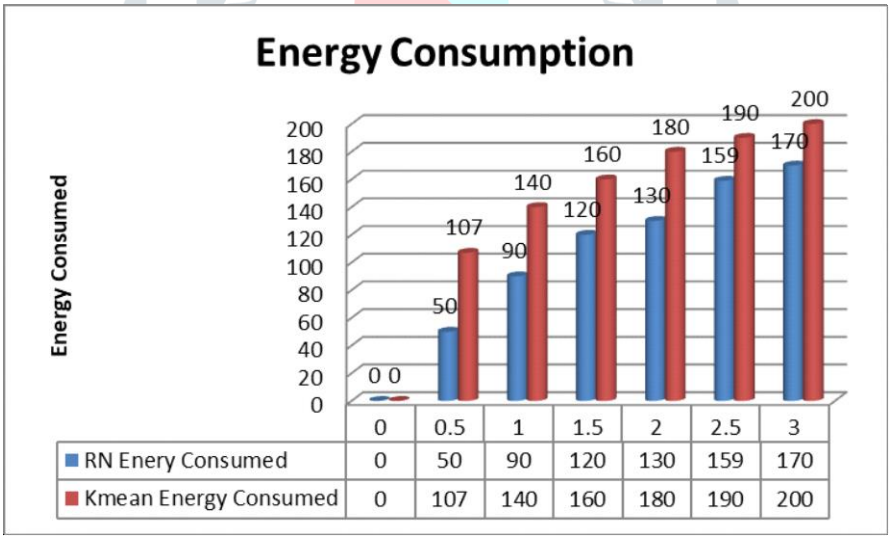


	0	0.5	1	1.5	2	2.5	3
RN Active Sensor Node	20	19	17	17	14	11	9
Kmean Active Sensor Node	20	17	15	12	9	7	3

Fig 5 Remaining Node Comparison Active Sensor Nodes

The comparison in fig 5 result shows with the increase in execution time the Active sensor in RN Method is better as compared to Kmean Method

2 Energy Consumed



	0	0.5	1	1.5	2	2.5	3
RN Enery Consumed	0	50	90	120	130	159	170
Kmean Energy Consumed	0	107	140	160	180	190	200

Fig6 Energy Consumption Comparison Active Sensor Nodes

The comparison in fig 5 result shows with the increase in execution time the Energy Consumption in RN Method is less as compared to Kmean Method

VI. CONCLUSION

In the proposed technique it is studied the basic parameters for a arbitrary disposition nodes detectors on the surveillance WSN applications, such as detecting an unauthorised intrusion in a specialist field. To improve the deployment quality and handle the issue of network coverage, an interference exposure model is proposed. As a result, detector node can sense each point in the detector network. When compared to the prior method, the intended strategy has a bigger number of vigorous detector nodes and lower energy usage as execution time increases.

REFERENCES

1 Navreetinder Kaur#1, Tarandeep Singh*2. "A Review of Wireless Sensor Network with Its Applications." International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016,pp 211-214

2 Prabhu, Boselin, and Sophia. "A Survey of Adaptive Distributed Clustering Algorithms for Wireless Sensor Networks." International Journal of Computer Science & Engineering Survey, vol. 2, no. 4, 2011, pp. 165–176

3 Gupta, C.p., and Arun Kumar. “Wireless Sensor Networks: A Review.” International Journal of Sensors Wireless Communications and Control, vol. 3, no. 1, 2013, pp. 25–36.,
4 Bal, R., Devi, G. and Nayak, S.,. " Node Deployment and Coverage in Wireless Sensor Network.". International Journal of Innovative Research in Advanced Engineering (IJIRAE),, vol 2, no. 1, 2014, pp.139-145.
5 Mao, Jia, et al. “Analysis of Node Deployment in Wireless Sensor Networks in Warehouse Environment Monitoring Systems.” EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, 2019 pp.1 -15 .
6 Poe, Wint Yi, and Jens B. Schmitt. "Node Deployment In Large Wireless Sensor Networks ". Asian Internet Engineering Conference On - AINTEC '09, 2009.
7 Dagdeviren, Orhan, and Vahid Khalilpour Akram. "The Effect Of Random Node Distribution And Transmission Ranges On Connectivity Robustness In Wireless Sensor Networks". 2019 International Symposium On Networks, Computers And Communications (ISNCC), 2019
8 Subir, Halder, et al. “A Lifetime Enhancing Node Deployment Strategy in WSN.” Future Generation Information Technology Lecture Notes in Computer Science, 2009, pp. 295–307
9 Khan, Wazir Zada, et al. “Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey.” International Journal of Distributed Sensor Networks, vol. 9, no. 5, 2013, p. 149023
10 Boudriga, Noureddine. “On a Controlled Random Deployment WSN-Based Monitoring System Allowing Fault Detection and Replacement.” International Journal of Distributed Sensor Networks, vol. 10, no. 4, 2014, pp. 101496.,
11 Assad, Noureddine et al. "Analysis Of The Deployment Quality For Intrusion Detection In Wireless Sensor Networks". Journal Of Computer Networks And Communications, vol 2015, 2015, pp. 1-7.
12 Zainol Abidin, Husna, and Norashidah Md. Din. "A Review on Sensor Node Placement Techniques in Wireless Sensor Networks". International journal on Advanced science engineering Information Technology ISRN , vol 2017, , pp. 190-197.
13 Sharma, Preeti, Monika Saluja2 and Krishan Kumar Saluja3 "A Review Of Selective Forwarding Attacks In Wireless Sensor Networks". International Journal Of Advanced Smart Sensor Network Systems, vol 2, no. 3, 2012, pp. 37-42. .
14 Zhang, Yuanyuan, and Marine Minier. "Selective Forwarding Attacks Against Data And ACK Flows In Network Coding And Countermeasures". Journal Of Computer Networks And Communications, vol 2012, 2012, pp. 1-14.
15 Hussain, Iftikhar et al. "Intruder Attacks On Wireless Sensor Networks: A Soft Decision And Prevention Mechanism". International Journal Of Advanced Computer Science And Applications, vol 10, no. 5, 2019 pp 609-617.
16 Surinder Singh, Hardeep Singh Saini. "Detection Techniques for Selective Forwarding Attack in Wireless Sensor Networks". International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-6S, March 2019.pp 380-383 .
17 Cho, Youngho, and Gang Qu. "Detection And Prevention Of Selective Forwarding-Based Denial-Of-Service Attacks In Wsns". International Journal Of Distributed Sensor Networks, vol 9, no. 8, 2013, p. 205920.