DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4598

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AN EFFICIENT APPROACH FOR ELIMINATING THE SYBIL, SINKHOLE AND WORMHOLE ATTACK IN WSN

Ekta Singh Parihar
Department of CSE/IT,
Madhav Institute of Technology & Science,
RGPV, Gwalior, India

Khushboo Agarwal,
Department of CSE/IT,
Madhav Institute of Technology & Science,
RGPV, Gwalior, India

Jaimala Jha
Department of CSE/IT,
Madhav Institute of Technology & Science,
RGPV, Gwalior, India

Abstract— A WSN having the extensive collection of sensor nodes which are able to sensing, processing and communicating they helps the base station to send and received information according to the situation in a meticulous environment. WSNs are susceptible in security area, there may be so many malicious activities are possible in the network. When some security attack occurs into the network, an IDS is used to distinguish the malicious nodes into the network as early as possible and generate some alert to take further action against malicious nodes. WSN is the extensive area of network, where lots of work done regarding security. Although, security is not fully preserve in WSN so in existing technique there are plenty of issues. By using Mac- duration they only recognize wormhole attack not all mention attack. This work done only when three way hand shaking happen but due to mobility network scenario change. There is no technique to prevent attacks. To resolve these difficulties, we performed some scenario to intercept the network from the wormhole, Sybil and sinkhole attack. In our proposed work, we take the threshold as an average value and compare it with mobility of nodes and drop count value simultaneously.

Keywords— WSN, Attacks, IDS, IPS, Mobile agents.

I. INTRODUCTION

WSN combine number of sensor nodes that are very small in size and act as sensing wireless devices, which densely expanded in various locations. These sensor nodes are conflict in sizes and include multiple sensing capabilities such as a radio transceiver for generating radio waves, microcontroller which controls the monitoring and various communicating devices. These several variety of sensor nodes performs different work in different fields efficiently. The exhaustive network contains the several types of sensors which sense the physical and environmental conditions and communicate themselves to gather global information [1].

Nowadays, smart environments represented by the revolutions in industrial, home and automation in transportation. Through WSN, data can be extractive for smart environments, where thousands of sensors are expanded at different locations and operating in different modes. A WSN is proficient for sensing, processing and communicating. These are very helpful to the base station or command node in any type of condition in a particular environment to observe and react. WSN protocols have a unique self-organizing capability. The sensor nodes are cooperative in nature this is the interesting feature of WSNs so they cooperate with each other. Before transmission raw data are processed by sensor nodes because they have an in-built processor. These features assist extensive collection of applications of WSNs, they vary from biomedical, environmental, military, event detection and vehicular telematics [2].

ATTACKS IN WSN

Wireless networks are more susceptible to security attacks than wired networks, because of the disseminate spirit of the conveyance medium. These attacks are ordinarily performed due to single or more vulnerability at the various layers in the WSN. Furthermore, sensor nodes are again and again situating in a unfriendly or unpredictable environment is an auxiliary penetrability of WSNs, where they are not physically conserved.

A. Sybil

Sybil attack is one of the types of attack in which spiteful node or device illicitly forging multiple identities of different nodes of the network. In Sybil attack, an adversary node can show off there appearance to be in diverse location at the common time. In other words, in the WSN sensor nodes falsify or thieving the identification of permissible nodes and presents multiple identities to other nodes.

B. Sinkhole (Blackhole)

In sinkhole attack, a spiteful node acts as a sinkhole to lure all the intercommunication service in the WSN. A spiteful node is established at the centre, which glance artistically to surrounding nodes and lures all the intercommunication service which put-up for a base station by the sensor nodes. Thereby, build a symbolic sinkhole with the antagonist at the center, which is possibly closer to the base station, from where

it can attract the most traffic, and the spiteful node could be perceived as a base station.

C. Wormhole

Wormhole attack is a prominent attack in which the attacker records the packets at one position in the network and tunnels those to variant position. In the wormhole attack, spiteful nodes monitor the packet and accept tunnel messages in one part of the network through a low latency link and retransmit them in a different part. This type of process generates a false scenario that the original sender is in the neighborhood of the distant place. The tunneling procedure forms wormholes in a sensor network. The tunneling or retransmitting of bits could be done selectively [3, 4].

II. RELATED WORK

Sepide Moradi, et al. (2016) presents that, a new method to detect Sybil attacks has been proposed. The method presented in this paper removes the adversary nodes from participation in routing while using mobile nodes and increases the security in network. The results of simulation demonstrate the proposed method has a good performance and does not impose additional overhead on the network while reducing packet loss rate [8].

Mrs.A.Vijayalakshmi, et al.(2016) present that, they have developed an simulated framework to evaluate the network loss probability as a performance metric for different distributed optimal movement strategies of mobile collectors moving over a graph (or network) for data harvesting in WSNs. Under this framework, they were able to find the Network coding strategy for the mobile collectors under mild conditions so as to minimize the network loss probability. Their optimal movement strategy can be made distributed using only local information via the Metropolis-Hastings algorithm. They have demonstrated through extensive numerical simulations that their Network coding strategy remarkably outperforms the Distributed optimal movement strategy under various settings of network topology, buffer size, and the number of mobile collectors, as well as heterogeneous and spatially-correlated data arrival patterns. They expect that their reasoning behind the Network coding strategy can be applicable for the design of Markova random walk based applications sample topologies of each sensor node [9].

Vladimir Shakhov, et al. (2016) present that, a consideration about special type of threats, which harm to the decadence of sensor battery power. In discrepancy to traditional DoS attack, quality of service under the measured attack is not necessary degraded. Moreover, the quality of service can be increased up to the crash moment of sensors set. Hence, the application of traditional defense mechanism against this threat is not always possible. Therefore, effective methods should be developed to counter the threat. They first discuss feasibility of rash depletion of battery power. Next, they proposed a model for evaluation of energy consumption under the attack. And counteracting technique against the attack is discussed as well [10].

Raksha Upadhyay, et al. (2015) present that, a solution to detect and prevent DDOS attack in WSN. The proposed mechanism will use the energy level for verification of spiteful node and its detection. As per the study, attacker deploys the spiteful node with extra battery capacity. Thus, after the complete communication they will be alive. Furthermore, malicious node will add extra processing load with data packets, so it will consume extra power at intermediate nodes [11].

Pengfei Zhang, et al. (2014) present that, a best possible event detection decision rules under Byzantine attacks for the first case and a newly low-complexity event detection algorithm based on Gaussian approximation and Moment Matching for the second case which contemplate a global decision. They evaluate their algorithms through extensive simulations. Simulation results demonstrate the Receiver Operating Characteristics (ROC) curves under special cases and scenarios, and therefore make available valuable upper bounds for various centralized and distributed designs. They also illustrate that their algorithms grant advanced detection execution when compared to local decision based schemes [12].

Babu Karuppiah, et al. (2014) presents that, the energy proficient incorporated Intrusion Detection System (IDS) to distinguish network layer Sybil attack. Their proposal spots out perfectly and exclude the Sybil node which may falsely act as a genuine node. The tentative results illustrate that the significant aspect in WSN, energy is preserved more proficiently by the proposed scheme than the existing alternative methods. Also, exact recognition of the spiteful node is probable spending rather less energy [13].

III. INTRUSION DETECTION AND PREVENTION SYSTEM

A. IDS

An intrusion detection system (IDS) is used to identify and to generate some alert when some intrusion activity is attempted into the system or network. IDS play an important role to recognize the spiteful nodes into the network as early as possible and generate some alert to get further action when some spiteful activities take place into the network. To detect intrusion, IDS dynamically monitor the system and the user actions in the system. Generally, three basic types of IDS are defined by different researcher's i.e. misuse detection, anomaly based detection and specification based detection. In misuse detection technique, some known attack signatures are to be compared to check the system vulnerability. Misuse based techniques are not effective to detect new attack because of lack of signature. So it requires updating the signature. Anomaly based IDS create normal profile of the system states or user behavior and compare them with current activities. If significant deviation occurs from the normal behavior of the node, IDS raise an alarm. The technique can detect new categories of attack but it is complicated to create exact normal profile. Another method, which merge anomaly and misuse detection techniques is known as specification based detection. This approach is based over manually developed specification. Both anomaly and specification based detection techniques

detect an attack by using deviation from a normal profile [5, 14].

B. IPS

In the network, intrusions and threats detected by IPS and the process of both detecting intrusion activities or threats and manage reactive actions on those called intrusion prevention system. IPS are monitoring real time packet traffic with spiteful activities or which match accurate profiles and will activate the making of alerts and it can drop, block that traffic in real time pass through in network. Generally, the IPS counter measures are to prevent an attack in progress. IPS can be termed as the addition of IDS with exercises of access control to defend computers from misuse. IPS is a smart device that does deserve not only detecting spiteful activities, but also to take defensive actions to protect the host. In simple terms, IDS may be completely suitable for network attack monitoring and for alerting administrators of emerging threats. Its speed, efficiency and limitations have formed a chance for IPS to challenge it as the dynamic protection of variety. The key functionalities performed by an IPS are as follows—

- IPS detects and takes preventive actions against spiteful attacks
- IPS stops the attack itself
- IPS changes the security environment
- IPS changes the attack's contents [6, 15]

C. MOBILE AGENT

A mobile agent is a different kind of application software or program that move among the nodes of a network to perform a tasks autonomously and intelligently way, in response to changing conditions in the network environment condition, to realize the objectives of the agent dispatcher. These types of agents have been found to be unique used in facilitating efficiently data fusion and dissemination in wireless sensor network. The traditional data transfer method that follows the client-server based paradigm, where the occurrences of certain events trigger surrounding source nodes to collect and send data to the sink individually. The client-server scenario, data in form of information transfer in general way is equal to how many the number of the source nodes in the given network, leading to bandwidth and power consumption. Furthermore, this approach could lead to unbalanced power consumption in the wireless sensor network the fact is that nodes near to the sink node transfer more data on behalf of other nodes. The sink node sends a mobile agent to the aim area to visit the source nodes in one to one way. The sensed information in form is less power consumption and aggregated by the agent and then sent back to the sink as instructed by the mobile agent, yielding a single traffic flow instead of multiple ones. There are also disadvantages of using mobile agents in scenario, such as code caching and with regard to different type of security issues [7].

IV. PROBLEM STATEMENT

WSN is one of the extensive area of network, where lots of work done regarding security. Although, security in not fully preserve in sensor network so in existing technique there are plenty of issues.

- By using Mac- duration we only identify wormhole attack not all mention attack.
- This work done only when three way hand shaking happen but due to mobility network scenario change.
- There is no technique to prevent attacks.

V. PROPOSED METHODOLOGY

To overcome these problems we introduced a new approach by which we identify attacks in network.
Wormhole attack: this is a data link layer attack by which two out band nodes communicate to each other and create a tunnel so that either they both drop the data or sense the data. So for prevent or detect this attack, we apply neighbor based network technique in which we get information of whole network by following three steps

- Get information of whole network scenario
- Update neighbor
- Mobility should be concern

Sybil attack: this is a Mac-layer attack, in which malicious node stole the identity of variant node, so that it easily acquire the data of other node to distinguish this attack, we follow three step

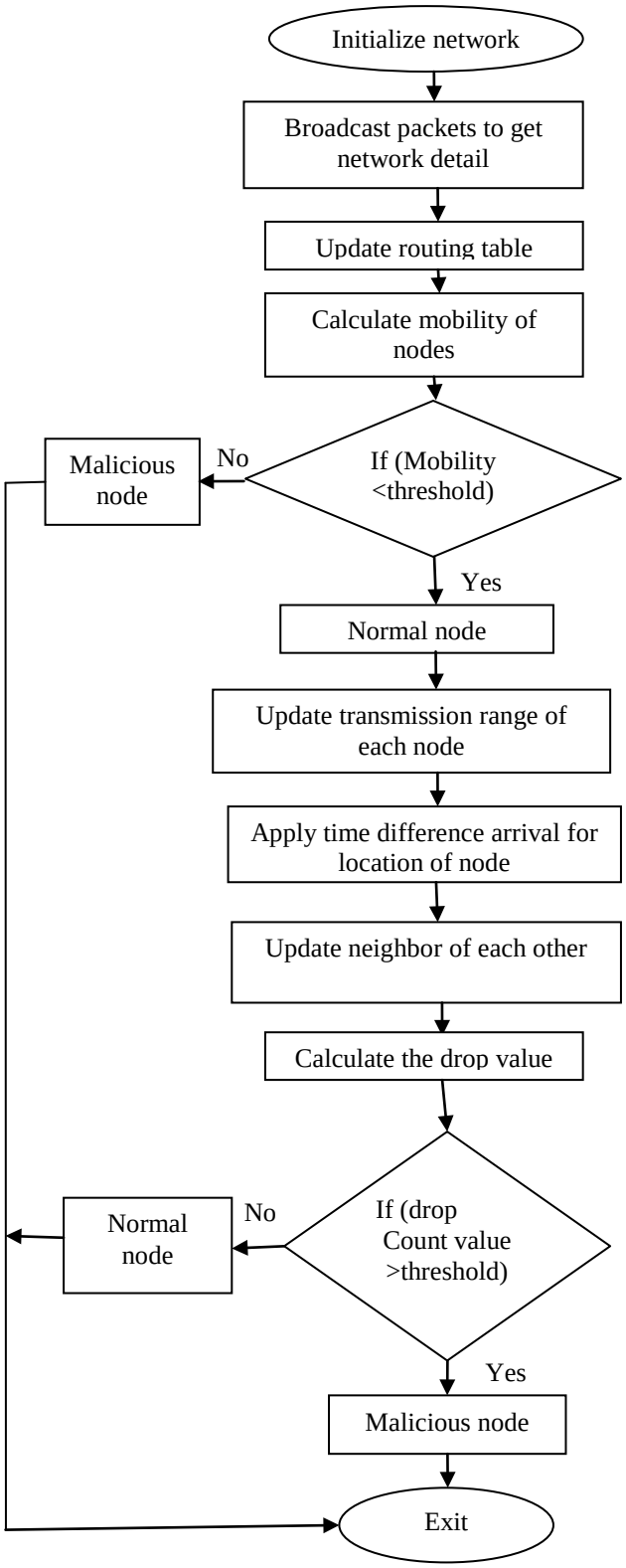
- Update node transmission range
- Update location of node using time difference arrival
- Update neighbor of each other.

Sinkhole attack: sinkhole attack simply drop the packet, so via newly approach we also find out sinkhole attack.

Expected outcome:

- Energy efficient
- Reliable transmission
- Network performance increase

VI. FLOWCHART



VII. PROPOSED ALGORITHM

Step:1 Initialization of network
Step:2 Broadcast the packets to get the network detail
Step:3 Update the routing table
Step:4 Calculate the mobility of nodes
Step:5 If (Mobility < threshold)
Normal node
Else
Malicious node
Step:6 Then update transmission range of each node
Step:7 Apply time difference arrival for location of node
Step:8 Update neighbor of each other
Step:9 Calculate the drop value
Step:10 If (drop count value > threshold)
Malicious node
Else
Normal node
Step:11 Exit

Here we use variable threshold, it used to calculate the threshold as an average value and compare it with the mobility and packet drop value simultaneously.

VIII. SIMULATION AND RESULT ANALYSIS

To examine the efficiency of our proposed system, we have Studied the system with a number of scenarios, Table 1 shows the simulation setup parameters. Fig. 1 demonstrates the initialization of network. Fig. 2 demonstrates the communication over the sensor nodes in the network. Fig. 3 demonstrates comparison analysis of the packet delivery ratio before and after the attack. Fig. 4 demonstrates the comparison of throughput after applying the new technique. Fig. 5 demonstrates the Routing overhead.

TABLE 1 Simulation Setup

Simulator:	NS2
Simulator Landscape:	1200x1000 (m^2)
Simulation Time:	100 (sec)
Node Transmission:	100 (m)
Network Size:	50 Nodes
Routing Protocol:	AODV
MAC Protocol:	802.11
Data Traffic:	CBR
Number of Attacker Nodes:	3

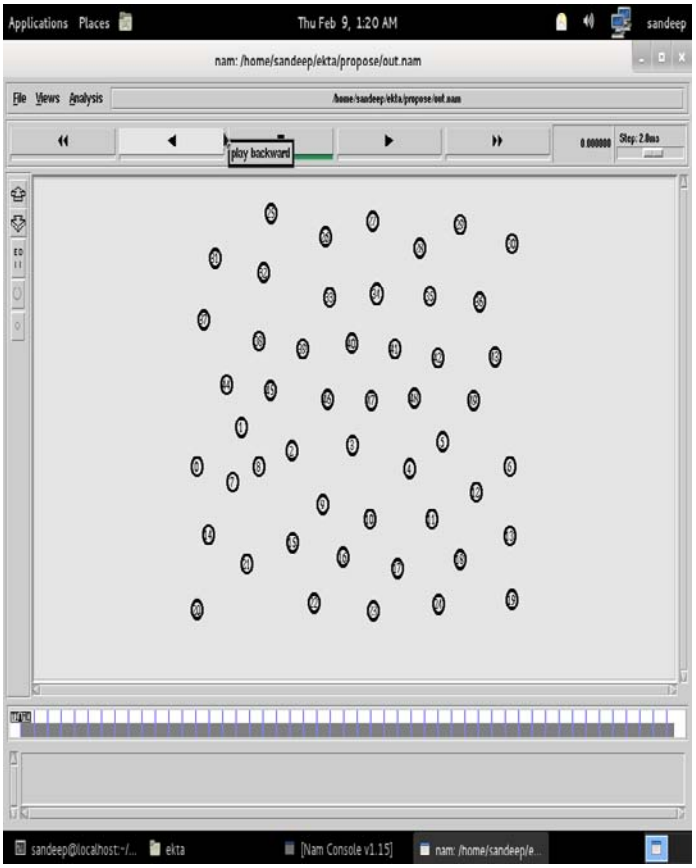


Fig. 1 Initialization of Network

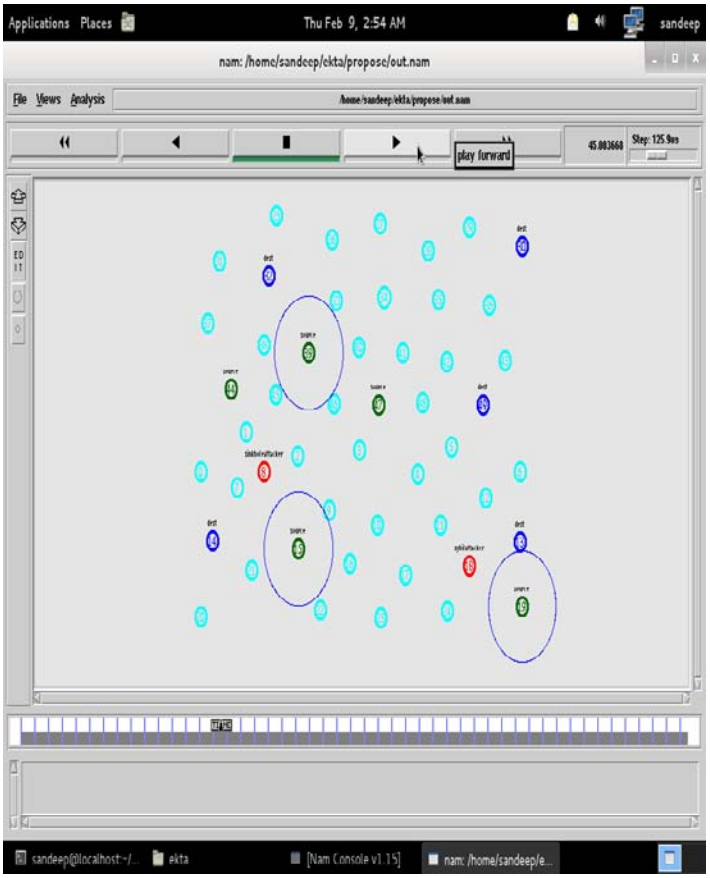


Fig. 2 Transmission Over the Nodes

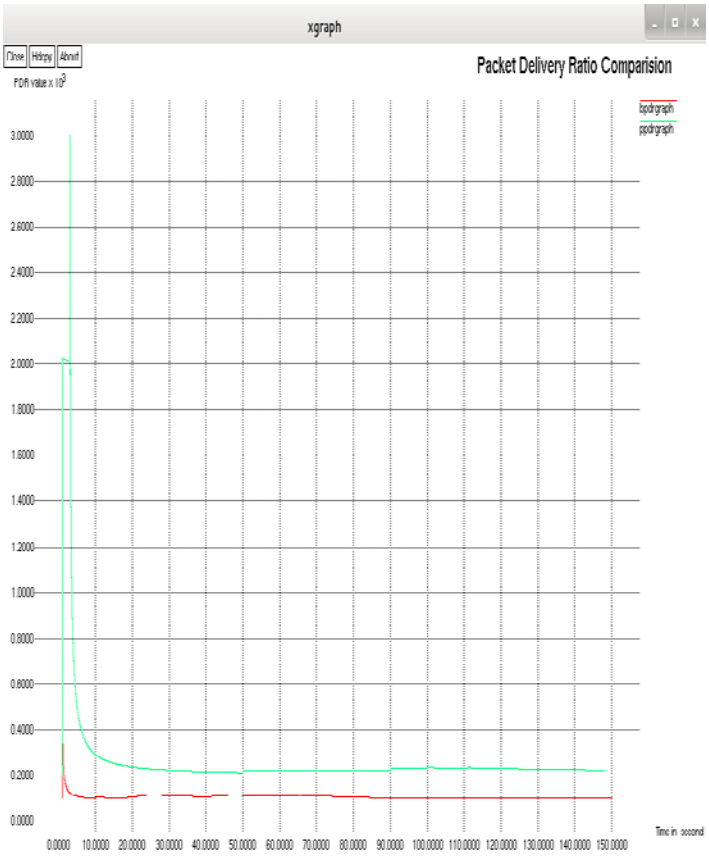


Fig. 3 PDR Graph

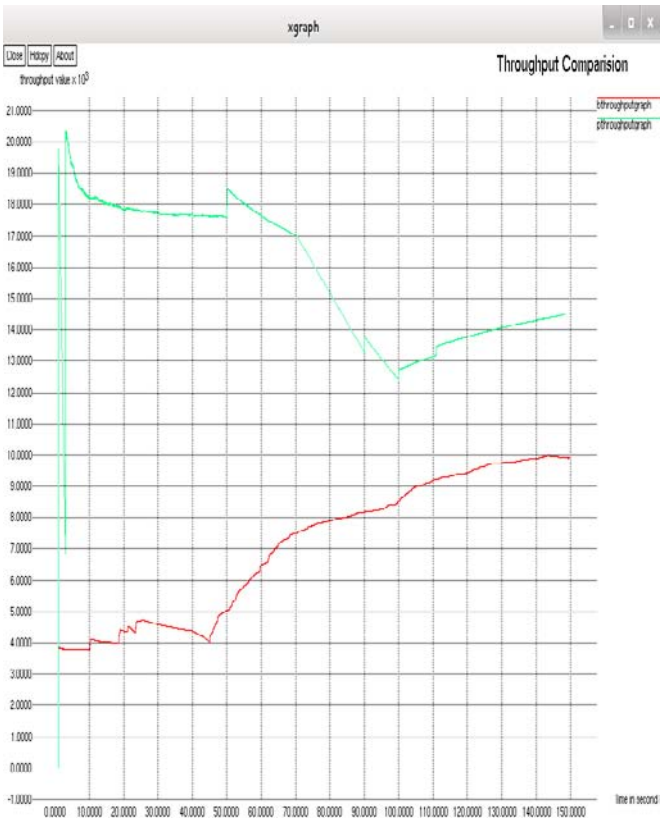


Fig. 4 Throughput Graph

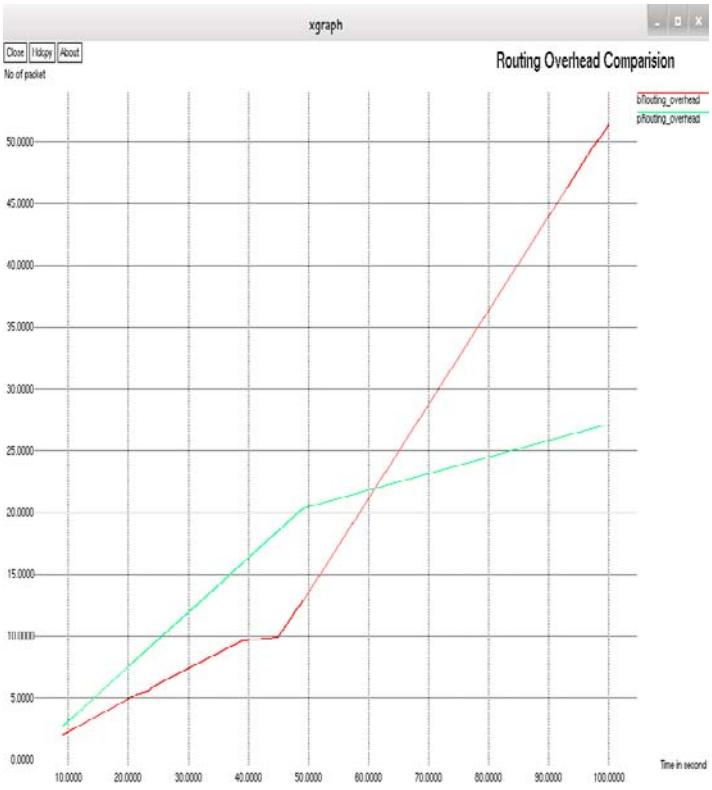


Fig. 5 Routing Overhead Graph

IX. CONCLUSION AND FUTURE WORK

In WSNs, the sensor nodes are expanded in unwrap and insecure province. So, the sensor networks are susceptible for multiple attacks such as sinkhole, wormhole and Sybil attack. In the existing technique, they have proposed a Mobile agent based IDPS to detect the attack by using cross layer approach. Cross layer may permit sharing of information among all of the five layers and moreover a layer has to determine its behaviour based over the data it accepts from other layers. Hence, we proposed a new technique which generate better result and boost the performance of the network.

In the future work, we can apply optimization technique to get the result in more accurate way for finding the malicious nodes in the network. We can also apply authentication process to perform the communication among the authenticated nodes.

X. REFERENCES

[1] B. Tamilarasi, R. Umarani, "Research Issues in Mobile Sensor Networks Applications and Survey of Key Factors", ISSN (Print) : 2319-5940, Vol. 2, Issue 6, June 2013 International Journal of Advanced Research in Computer and Communication Engineering.

[2] Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, And Elijah Blessing Rajsingh, "Research Issues In Wireless Sensor Network Applications: A Survey", International Journal Of Information And Electronics Engineering, Vol.2, Issue.5, September 2012.

[3] Shio Kumar Singh, M P Singh, And D K Singh, "A Survey On Network Security And Attack Defense Mechanism For Wireless Sensor Networks", ISSN: 2231-2803, Nternational Journal Of Computer Trends And Technology- May To June Issue 2011.

[4] Ms. Anjusree.S, Mrs. V.Praveena, "A Relative Study For Detection And Prevention Of Ddos Attacks", ISSN(Online): 2320-9801, Vol.1, Issue. 8, October 2013, International Journal Of Innovative Research In Computer And Communication Engineering.

[5] Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Moutushi Singh, Souvik Sarkar, Jamuna Kanta Singh, And Koushik Majumder, "Intelligent Intrusion Detection System In Wireless Sensor Network", pp.707-712, 10.1007/978-3-319-12012-6_78, (FICTA) 2014.

[6] Nilotpal Chakraborty, "intrusion detection system and intrusion prevention system: a comparative study", ISSN (Online) : 2229-6166, Vol.4, Issue.2, May 2013, IJCBR.

[7] Min chen, Sergio gonzalez, and victor c. m. leung, "applications and design issues for mobile agents in wireless sensor networks", 1536-1284/07© 2007 IEEE.

[8] Sepide Moradi, Meysam Alavi, "A Distributed Method Based On Mobile Agent To Detect Sybil Attacks In Wireless Sensor Networks", 978-1-5090-4335-4/16/$31.00 C 2016 IEEE.

[9] Mrs.A.Vijayalakshmi, V.Bhuvaneswari, "Mobile Agent Based Optimal Data Gathering In Wireless Sensor Networks". **ISBN:** 978-1-4673-7807-9, **Number:** 16429457, 7-8 Jan. 2016 IEEE.

[10] Vladimir Shakhov, "On A New Type Of Attack In Wireless Sensor Networks: Depletion Of Battery", 978-1-5090-0855-1/16/$31.00 ©2016 IEEE

[11] Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt, "Detection And Prevention Of DDOS Attack In WSN For AODV And DSR Using Battery Drain", 978-1-4673-7309-8/15/$31.00 ©2015 IEEE

[12] Pengfei Zhang , Jing Yang Koh , Shaowei Lin , Ido Nevat, "Distributed Event Detection Under Byzantine Attack In Wireless Sensor Networks", 978-1-4799-2843-9/14/© 2014 IEEE

[13] Babu Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, Al-Sakib Khan Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm For Intrusion Detection System In Wireless Sensor Networks", 978-1-4799-7002-5/14 $31.00 © 2014 IEEE.

[14] Khushboo Agarwal, Vikas Sejwar "Effect on Throughput due to Changes in Transmission Power of Nodes in MANET" in IJFGCN, Vol.8, Issue 3, 2015, Pg 207-212.

[15] Ekta Singh Parihar, Khushboo Agarwal, Jaimala Jha "A Theoretical Review On Multiple Security Threats in The Wireless Sensor Network" International Journal for Science and Advance Research In Technology Vol.3 , Issue 8 , August 2017