A Reserve Path based Black Hole Detection and Prevention Algorithm in Wireless Sensor Network

Rajvir Kaur
Computer Science and Engineering
LLRIET,
Moga, India

Harpreet Kaur
Computer Science and Engineering
LLRIET,
Moga, India

ABSTRACT
Due to various characteristics of WSN, network is too unsafe and open for malicious attacks. Attackers can easily comprised an attacking node that causes information loss and network degradation. Numbers of solutions are cumbersome and vitality inefficient. In this paper a novel approach has been proposed for detection and elimination of black hole attack comprised nodes. Proposed approach is based on threshold value and reverse tracking process for detection and elimination of malicious node. TDMA policy has been used for transmission of information from a cluster to sink node. Results show that proposed approach is much efficient rather than that of previous one.

Keywords
AODV, Black Hole, Security Goals, WSN

1. INTRODUCTION
WSN is the field on networking that utilized various types of nodes for sensing information from the sensing environment. In the process of WSN various nodes have been deployed under a particular region so that information can be sensed from that region. Sensor nodes are responsible for data sensing based on various types of sensors. Sensor nodes comprise various parts for functioning towards sensing and transmitting information. These different parts for functioning of sensing nodes are sensor, battery, transmitter, receiver and memory device. In the processing of WSN sensing nodes has been disbursed in a particular region for environment sensing and data processing. BS has been responsible for data collection from the sensor nodes using routing strategy and that received data has been used for decision making process.

WSN consumes energy from the sensor nodes under different operations performed by these nodes. Power consumption is major issue related to wireless sensor network from past research. Since a large number of routing protocols have been developed for routing in such a way that minimum energy can be consumed by the network. In past decade's chain based routing protocols had been emerged to overcome issue of power utilization over the network. Cluster formation has been evolved a best way that has been adopted by multiple routing protocols for minimization of energy utilization over the network.

Attack Vern-ability is major security threat in WSN that degrades performance of network and data leakage to unauthorized organizations. Attacks have been mostly made on the network layer and routing layer to fluctuate routing path of the data message so that information integrity can be easily changed. Most harmful attacks that prone to WSN are black-hole attack, gray-hole attack and sink-hole attack. Black hole attack comprises itself as the agent node that can easily attack data traffic from sink nodes of sensor nodes. The adversary node available in the network comprises itself as the shortest route for data transmission to sink node and collect all the information so that data integrity can affected.

1.1 WSN Security Goals
i. **Data Confidentiality:** It is the ability to hide message from a passive attacker and is the most important issue in network security. Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a WSN. Moreover, sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack.

ii. **Data Integrity and Authentication:** Integrity refers to the ability to confirm the message has not been tampered or altered while it was on the network. An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Indeed, data authentication allows a receiver to verify that the data really is sent by the claimed sender.

iii. **Time synchronization:** wireless time synchronization is used for many different purposes including location, proximity energy efficiency and mobility to name a few.

iv. **Freshness:** WSNs provide some measurements in time. We must ensure that each message is fresh. The freshness of data implies that the data are recent, and it ensures that no adversary replay the old messages.

v. **Access control:** gives to the legitimate participants a means to detect the messages coming from external sources of the network Availability: the availability gives insurance over the network and time of response of the system to transmit information from sink node to destination node.

2. RELATED WORK
Karakehayov Z.(2005) presented, a novel routing algorithm utilized for forward packets of geographic routing with help of two broadcast messages MISS and SAMBA, to protect a distributed database for detected black hole attacks in WSN MISS (material for intersection of suspicious sets) message used to identify malicious node in network using ID space. SAMBA (suspicious area, mark a black hole attack) messaged detected location of black hole attacked using physical space. Security overhead declined the network's vulnerability at the expense of more energy drawn from batteries of involved nodes. REWARD (Receive, Watch, Redirect) allows to strike the balanced between lifetime performance and security capability. This technique worked well at different levels of security which could be set according to the local conditions. The analyzed the energy overhead associated with different REWARD modifications. [15]

Gondwal N. and chander D. (2013) worked upon the wireless nature and infrastructure-less environment of WSN. They were more vulnerable to many types of security attacks. This paper proposed a technique to detect the black-hole attack using multiple base-stations and a check agent based technology. This technique was Energy efficient, Fast, Lightweight and used for Reduces message complexity. An effective solution was proposed that it uses multiple base stations to improve the delivery of the packets of the sensor nodes, reaching at least one base station in the network, thus ensuring high packet delivery success. The proposed technique was more efficient than the previous techniques and gives better results. Check agent was a software program which was self-controlling and it moved from node to node and checks the presence of black-hole nodes in the network. Routing through multiple base stations algorithm was only activated when there was a chance of black-hole attack on the network. [12]

Karuppiah et al. (2015) studied an improvised hierarchical vitality efficient intrusion detection system was proposed, to protect sensor Network from black hole attacks. Previous approach was simple and was based on exchange of control packets of sensor node and base station in WSN. The results show that proposed algorithm was effective against detecting and preventing efficiently the black hole attacks. [16]

Priya and Puri (2015) Studied the mobile Ad-Hoc Networks had the ability to deploy a network where a traditional network infrastructure environment could not possibly be deployed. In the approach had analyzed the behavior and challenges about security threats to mobile Ad-Hoc networks implemented the Conniver broadcasting node Technique mode in a better way. Many solutions had been proposed, but these solutions were not perfect in terms to effectiveness and efficiency. If any solution works well in the presence of single malicious node, it could be applicable in case of multiple malicious nodes. After referring multiple approaches and applying Conniver broadcasting node technique mode after the detection of selective black hole attacked would surely decrease the rate of loss in data packet. More ever, the Conniver broadcasting node Technique modes were applied only for nodes that were attacked, rather for applying for all the nodes. Hence loss of energy was surely avoided. [14]

R. Mohamed et al. (2015) employed the intrusion detection system against Sink-Hole attack in wireless sensor networks with mobile sink. The Intrusion Detection System (IDS) against Sinkhole attack in wireless sensor networks with mobile sink. In the detection model, the network area was divided into a flat grid of cells, and used the signature-based technique, which was represented by the detection rate of a cell, to distinguish between real and fake sink nodes. The proposed IDS consider two types of sink mobility: periodic and random. In addition, the cell leaders do not activate their IDS agent simultaneously; the additional energy consumption incurred by the IDS was low. Simulation results show the efficiency of proposed IDS in terms of detection rate, efficiency, and energy consumption. [13]

Tanuja et al. (2005) described the security allowed WSN to be used data onto node to node with confidence and maintain integrity. Without security, the result would be undesirable consequences. Security must be addressed to critical sensor applications. The proposed algorithm used to overcome black hole node and false data injection attack in WSN. To simplify the elimination of black hole and guaranteed successful delivery of packet of source of destination by used a new acknowledgement schemed against low overhead. The algorithm could eliminate false data injection by outside malicious nodes. Simulation resulted shown that algorithm could successfully identify and eliminate hundred percentages black hole nodes and ensured more than Ninety nine percentage packet delivery of increased network traffic. [21]

3. PROPOSED WORK

In the scenario of WSN nodes have been localized in a particular region for sensing information. The attacker available performs different types of attackers over the network to degrade the performance of the network. In the purposed work black hole attack detection has been done using reverse tracking mechanism.

3.1 Detection and elimination of malicious nodes

In the purposed work attacker introduce sink node in the network and sink nodes broadcast RREQ for collection of data and sensor nodes does not aware about authentication of the sink nodes available in the network. These nodes transmit this information to the sink node. Attacker can transmit this information to attacker base station or can falsify the information and transmit to base station so that wrong decision can be made. On the basis various detection approaches black hole attack can be detected from the WSN. In the purposed work reverse tracing mechanism has been used for detection of attacking node available in network. Time division multiplexing has been used for data transmission over the network and RREQ and RREP has been used for detection of possible paths for data transmission over the network. Due to utilization of TDMA genuine nodes will transmit broadcast message for data collection. If any node broadcast message out of particular time stamp that will treated as malicious node. Threshold based acknowledgement has been used that utilize reverse tracking mechanism and verify the path under attack or not. On the basis of these reverse tracking process nodes that are under attack has been detected and eliminated by not utilizing particular path for data transmission over the network to base station. Base station collects all the information and utilize for decision developing process.

3.2 Work Flow

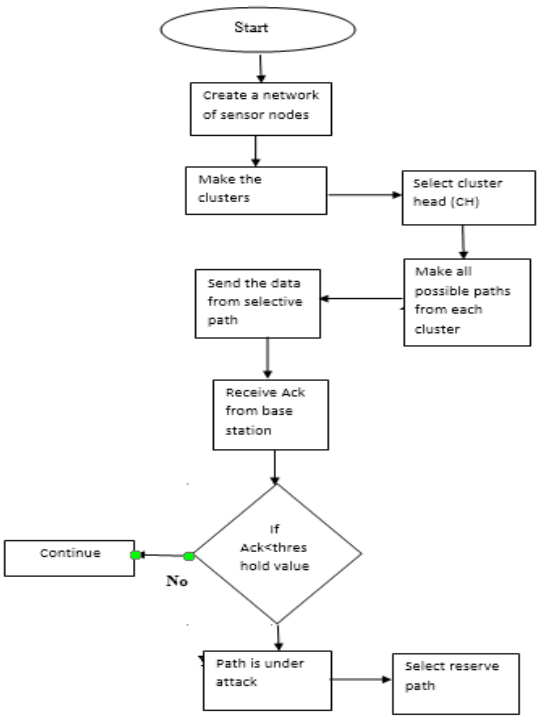

Figure 1: Work Flow of Proposed Work

Figure 1, represents the flow of the purposed work for malicious node detection. In the purposed work sensor nodes have been provided a timestamp for broadcasting message for transmission of data. Sink nodes available in the network broadcast message to all sensor nodes for collection of data. Nodes will transmit request within timestamp that has been defined by the trusting authority. In the purposed work AODV routing protocol has been used for transmission of data. Malicious node changes the route table strategy of AODV that transmit request to all nodes that comprised node contain a shortest path for data transmission to base station. To detect black hole attacking node available in the network reverse tracking path has been utilized.

3.3 Pseudocode for the Proposed Work

The various steps that are followed are as follows:

i. Establish a Network of sensor nodes.
ii. Divide the Entire network of clusters of selecting a cluster head.
iii. Select all possible paths of communication with transceiver.
iv. Check the health for path before sending the data and compare it with thresh hold value.
v. IF
   a. health >= threshold values
      Communication could be held via same path.
   b. health < threshold values
   c. Select reserve path to detection of malicious nodes.
   d. Check one-hop neighbor nodes via transmitting single bit message.
   e. If RREP from one- hop neighbor
      Genuine node, data can be transmitted
   f. Else
      Reply from other node detect node id and comprised as malicious node
   End if

4. RESULTS AND DISCUSSION

Sensor nodes have been deployed in the environment for capturing information. These nodes capture information from particular environment and transmit this information to base station. Various parameters have been used in WSN for sensing information. These nodes consume energy while sensing, receiving and transmitting information.

Table 1: Simulation Parameters

Network Parameters	Values
Number of Nodes	100,50
Agent	TCP/TCP-Sink
Routing Protocol	AODV
Antenna Type	Omni
MAC Type	802.11
Queue Type	Drop Tail
Queue Length	50
Simulation Time	50s
Traffic Type	CBR
Energy Model	Energy Model
Transmission Energy	0.9 J
Receiving Energy	0.5 J
Initial Energy	50 J

Table 1, represents various parameters that have been used for simulation of proposed work under network simulator. On the basis of these different simulation parameters wireless sensor network has been designed and used for data sensing and transmission over the network. Routing protocols are responsible for data transmission from possible paths available in the network.

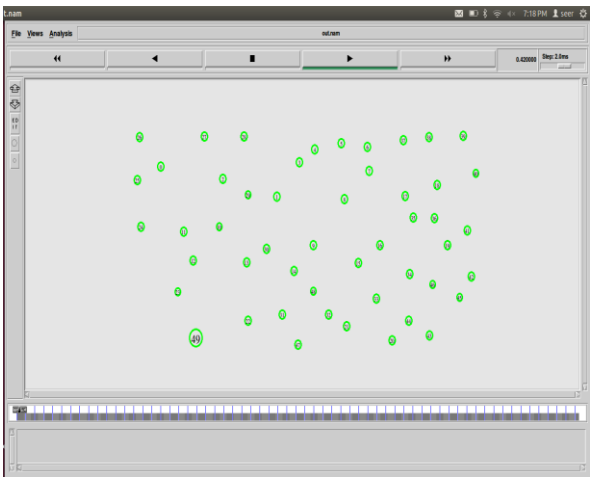

Figure 2: Initialization of Nodes

Figure 2 represents initialization of wireless sensor network for sensing information from environment. In WSN nodes sense information from a particular environment and transmit information to base station for decision making process.

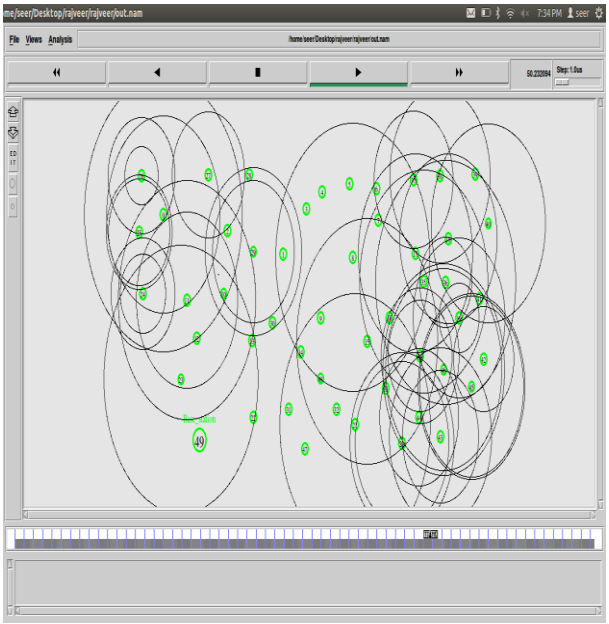

Figure 3: Routing between nodes

Figure 3 is representing the Routing between the nodes. Each and every node communicates with one-another. One node sends the message to other nodes and the receiver node responds to the sender node according to the message received.

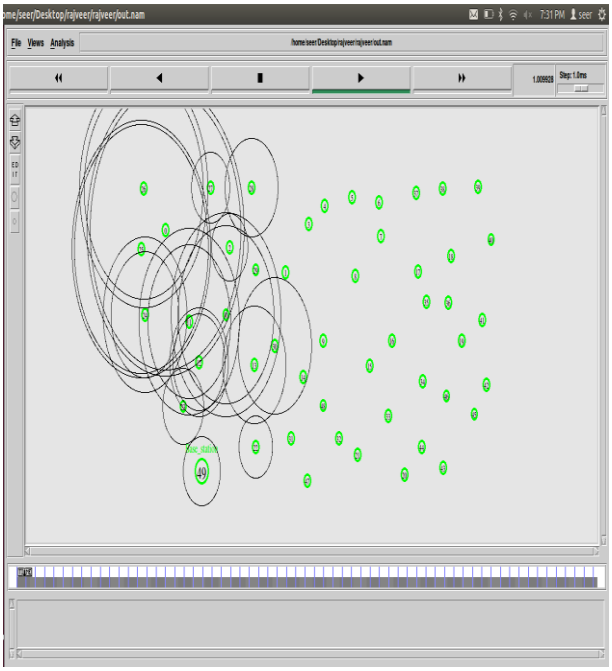

Figure 4: Cluster division and Data transmission

Figure 4 represents the various clusters which have been formed over the network and the cluster which have been used for data transmission from sensor nodes to the base station. In the proposed work TDMA has been used for data transmission to base station using different nodes available in the network.

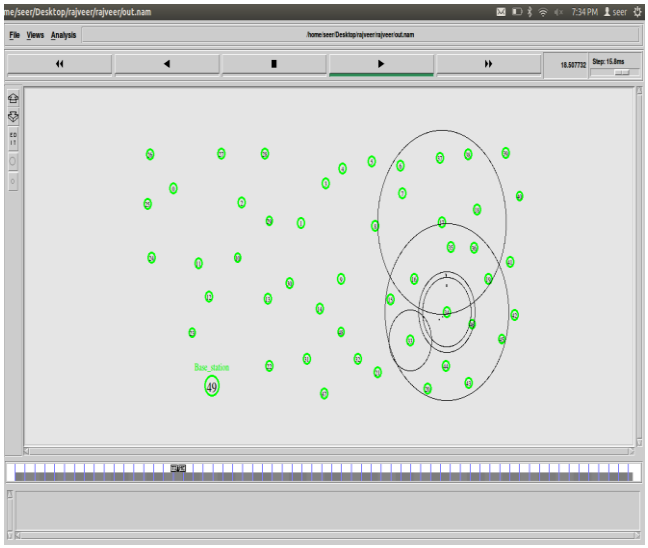

Figure 5: Reverse Tracking Mechanism

Figure 5 represents compromised nodes which makes use of routing metric to lie to its neighbors in order to launch sinkhole attack. Then all the data from his neighbors to base station will pass through compromised node. In this actual data doesn't receive at base station that loss the information of the network. Here, the black hole attack detection scheme has to be implement that detect attacking node and provide reliable information. This has been done by using reverse tracking process and if the data received by the base station is less than that of the transmitted node by a threshold value than the particular path has been known as blacklisted path and other path has been selected for data transmission.

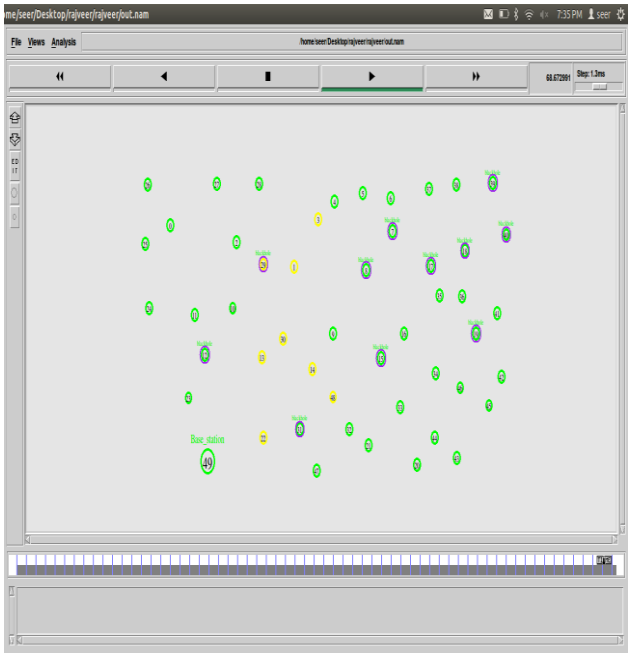

Figure 6: Detection of black hole Attack

Figure 6 shows the reverse tracking path mechanism, on the basis of which various paths that has been used for data transmissions have been black listed. After this process a one hop neighbor mechanism has been used for detection of nodes that encounters black hole attack over the network. These nodes have been detected using single neighbor detection approach. In this process node broadcast a message to single hop neighbor with hop id 1.

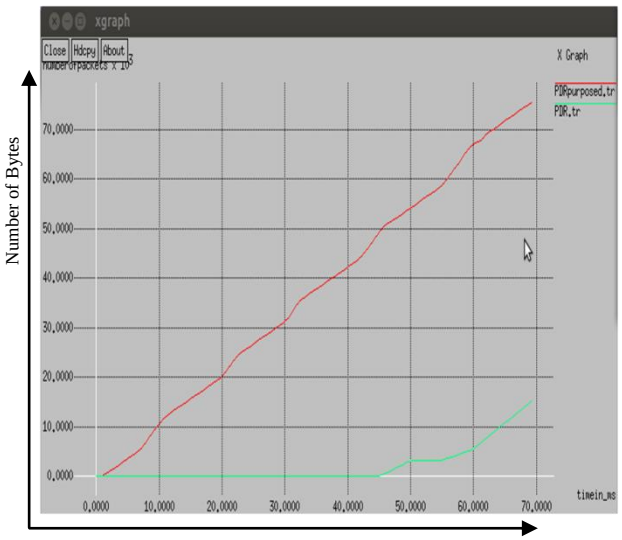

Figure 7: Packet Delivery Ratio

Figure 7 shows the Packet Delivery Ratio, which is defined as the number of packet deliver with respect to time. The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace file. In general, PDR is defined as the ratio between the received packets by the destination and the generated packets by the source.

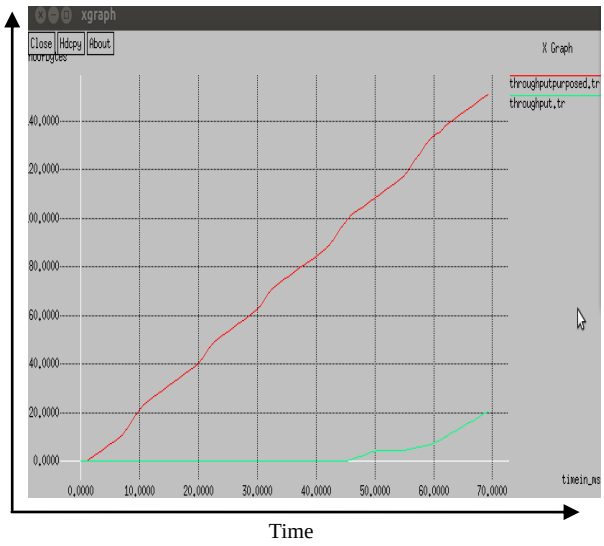

Figure 8: Throughput

Figure 8 represents the Throughput. Throughput is defined as the number of packet delivered successfully over the network. Throughput represents bytes transmitted per unit time. In general terms, throughput is the maximum rate of production or the maximum rate at which something can be processed. When used in the context of communication networks. It is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps). This graph represents comparison between proposed and AODV routing protocol.

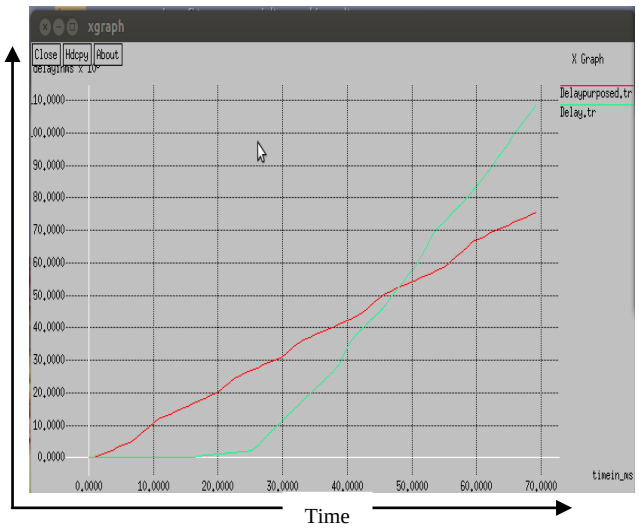

Figure 9: Packet Delay

Figure 9 is showing the graph of Packet Delay. Packet Delay is defined as the Delay between packets during transmission. In this graph delay has been measure for purposed and previous approach. Delay has been measured in terms of time units.

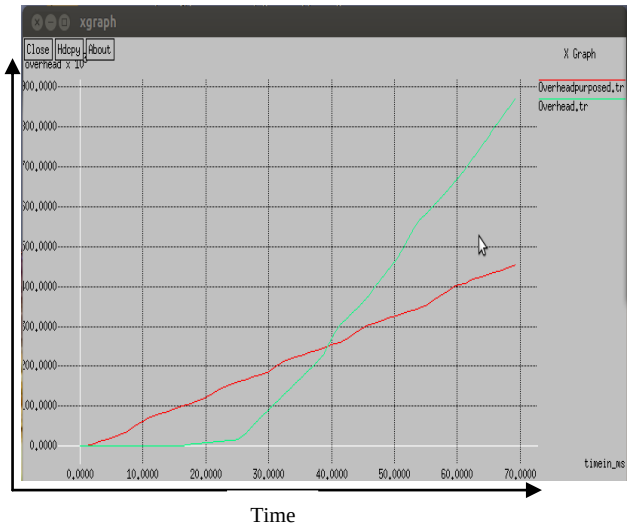

Figure 10: Overhead

Figure 10 is representing the network overhead. Overhead has been caused due to routing packets that has been transmitted over the network. Overhead cause various problems over the network.

5. CONCLUSIONS

In this paper black hole attack detection has been done that has been attacked by any attacker by developing a compromised node in WSN. The attackers introduce the node in the network that advertises for data collection from sensor nodes and transmit data to wrong destination. In the purposed work black hole detection has been done on the basis detection algorithm that utilized reverse tracking strategy

On the basis of reverse tracking mechanism nodes that comprised attack has been detected during reverse tracking process based on different one hop neighbor detection. On the basis of this detection malicious nodes have been eliminated from network to participate under communication process that concludes that information loss is less and data integrity is assured. On the basis of these parameters that are throughput, packet delivery ratio, overhead and delay one can conclude that purposed work provides much better results than previous approaches.

6. FUTURE SCOPE

For the future reference, mobility based WSN can be used for detection of attacking nodes in WSN. Proposed work does not provide much accuracy during mobile wireless sensor network. Due to mobility path of the nodes, detection is not an easy process. That problem can be mitigating by developing IDS for all type of WSN.

7. ACKNOWLEDGEMENTS

First of all I am grateful to **The Almighty God** for establishing me to complete this dissertation.

I'm highly indebted to a number of individuals in academic as well as in social circle who have contributed to this thesis. In particular, I wish to extend my appreciation to my supervisor ***Er. HARPREET KAUR, Assistant Professor at Lala Lajpat Rai Institute of Engineering and Technology, Moga***, who has the attitude and substance of a genius. She continually and

convincingly conveyed a spirit of adventures in regard to research and an excitement in regards to teaching. Without her guidance and persistent help this dissertation would not have been possible. Her valuable and expert supervision, attention grabbing views and obliging nature led to successful completion of this work.

I would like to take this opportunity as a special note of thanks to my parents and friends for their unceasing encouragement and support. I would not have been able to complete this thesis without their motivation.

Last but not the least; I would like to thank one and all who, directly and indirectly, have lent their helping hand in this venture and supported me in the completion of this thesis.

8. REFERENCES

[1] A. Vijayalakshmi, T. Shrimathy and T. G. Palanivelu, "Mobile agent middleware security for Wireless Sensor Networks,"*2014 International Conference on Communication and Signal Processing*, Melmaruvathur, 2014, pp. 1669-1673.

[2] S. Ahmad Salehi, M. A. Razzaque, P. Naraei and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks,"*2013 IEEE International Conference on Space Science and Communication (IconSpace)*, Melaka, 2013, pp. 361-365.

[3] C. T. Hsueh, C. Y. Wen and Y. C. Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks," in *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3590-3602, June 2015.

[4] Debiao He, N. Kumar and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,"*International Symposium on Wireless and pervasive Computing (ISWPC)*, Taipei, 2013, pp. 1-6.

[5] M. Guerroumi, A. Derhab and K. Saleem, "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink,"*2015 12th International Conference on Information Technology - New Generations*, Las Vegas, NV, 2015, pp. 307-313.

[6] R. Geetha, S. R. Anand and E. Kannan, "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks,"*International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, 2014, pp. 1-6.

[7] Guanglai Chen, Shoujun Wang and Lifei Li, "Notice of Retraction
The design of wireless wave height sensor network node based on Zigbee technology,"*2011 International Conference on Electric Information and Control Engineering*, Wuhan, 2011, pp. 3683-3686.

[8] H. Chen, Z. Han and Z. Fu, "Quantitative Trustworthy Evaluation Scheme for Trust Routing Scheme in Wireless Sensor Networks," *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, 2015, pp. 1272-1278.

[9] I. Makhdoom, M. Afzal and I. Rashid, "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks,"*2014 National Software Engineering Conference*, Rawalpindi, 2014, pp. 1-6.

[10] J. Krithiga and R. C. Porselvi, "Efficient CodeGuard mechanism against pollution attacks in interflow Network coding,"*2014 International Conference on Communication and Signal Processing*, Melmaruvathur, 2014, pp. 1384-1388.

[11] R. Mittal and M. P. S. Bhatia, "Wireless sensor networks for monitoring the environmental activities,"*2010 IEEE International Conference on Computational Intelligence and Computing Research*, Coimbatore, 2010, pp. 1-5.

[12] N. Marriwala and P. Rathee, "An approach to increase the wireless sensor network lifetime,"*2012 World Congress on Information and Communication Technologies*, Trivandrum, 2012, pp. 495-499.

[13] R.Muhammad and H.Syed Irfan ,"A force routing information modification model for preventing black hole attacks in wireless adhoc network " , IEEE 2011.

[14] Priya and Puri *"Remove of selective black hole attack with upstream node and downstream node alarm system by dynamic source protocol (DSP)"* International journal of advanced engineering technology Vol.5, No. 5,2015,

[15] Karakehayov (2005)."*Using REWARD to detect team black-hole attacks in wireless sensor networks*" International Journal of Innovative Research in Science Engineering and Technology.

[16] Karuppiah, Dalfiah and R. Yuvashri*,"An improvised hierarchical black hole detection algorithm in wireless "*international conference information in computing technologies (ICIICT), Chennai, India 2015.

[17] Ahmed, S. and Sanjay, "The holes problem in wireless sensor network" mobile computing and communications review, Vol.1, No.2, 2014.

[18] G. Nitesh and D. Diwaker,"*Detecting blackhole attack in wsn by check agent using multiple base stations*", American International Journal of Research in Science, Technology, Engineering & Mathematics, 2013

[19] R.K, Prakash and Mishra "*A Review on Black Hole/Sink Hole Attack Detection and Prevention in WSNs"* International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 5, Issue 6,2015

[20] B.R. and V.N. *"Black hole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms*" International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, 2014.

[21] Tseng, Chou And Chao"*A survey of black hole attacks in wireless mobile ad hoc networks*" Human centric computing and information sciences. 2011.