International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

Collaborative Decision for Wormhole Attack Prevention in WSN

M.Tech. Scholar Rajani Kant Tiwari, Assistant Professor Devkant Sen
Department of Electronics & Communication
Technocrats Institute of Technology & Science Bhopal(M.P), India
Rajanikant960@gmail.com,Devkantsen1984@gmail.com

***Abstract* – The dynamic network called WSN is very popular for short range communication between the mobile devices. This research is very useful in field of security to evaluate the network performance in case of attack and proposed previous security scheme. Due to the absence of centralized administration, security is the main issue in WSN and attackers are very easily modified the actual behavior and performance of network. The wormhole attack is creating the tunnel. In this attack two or more malicious colluding nodes create a higher-level virtual tunnel in the network, which is employed to transport packets between the tunnel endpoints. These tunnels emulate shorter links in the network and so act as benefit to unsuspecting network nodes which by default seek shorter routes. In this paper we proposed a scheme against wormhole attack. Worm hole attack is a type of attack that are work as to established path in between sender and receiver but if the sender has start data transmission then in that case the worm hole attacker has create a direct link, referred to as a wormhole tunnel between them and all the data pass through that tunnel. In this research we proposed Wormhole attack Intrusion Detection as well as prevention (IPS) Security Scheme against wormhole attack. For detection we identified the information of intermediate nodes and get attacker node information like node number, number of attacker and infected packets it means trustful communication among the nodes by that the higher successful data communication process rates may well possible. After that we prevent wormhole attack using broadcasting the particular identification (ID) of attacker by that no node in network replies of that request and secure the mobile ad-hoc network communication.**

***Keywords*– Wormhole, attack, IPS, WSN, Routing, Security.**

I. INTRODUCTION

WSN is considered an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. They also have capability of network partition [1]. A Wireless Sensor Network (WSN) is a self-organized multi-hop system comprised of mobile wireless nodes. Two nodes out of direct communication range need intermediate nodes to forward their messages. These networks are independent of any fixed infrastructure or central entity like cellular networks [2] which requires fixed infrastructure to operate. The nodes in WSN may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes. Due to this absence of authority, conventional techniques of network management and security are scarcely necessary for WSN. Any attacker or malicious node in the network can disturb the whole process or can even stop it. Several attacks like, wormhole, rushing etc [2] have been come into the picture under which a genuine node behaves in a malicious manner. It is quite difficult to define and detect such behavior of a node. Therefore, it becomes mandatory to define the normal and malicious behavior of a node. Whenever a node exhibits a malicious behavior under any attack, it assures the breach of security principles like availability, integrity, confidentiality etc [2]. An intruder takes advantage of the vulnerabilities (which is discussed in next section) presents in the sensor network and attacks the node which breaches the security principles.

In a wormhole attack [2, 3] an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point mentioned in figure 1. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example, through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole

directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself by that all packets are forwarded through tunnel and actual destination only wait for data. In world, such an unselfish angle is quite typically extraordinarily troublesome to appreciate and then we regularly notice malicious nodes conjointly contribution within the same network. A number of these are alien nodes that enter the network throughout its establishment or operation section, whereas others might originate indigenously by compromising an existing benevolent node. These malicious nodes will perform each Passive and Active attacks against the network mention in next section.

II. ATTACK AND SECURITY ISSUE IN WSN

There are two kinds of attacks in WSN [4, 5] first is passive attack and another is active attack. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. .

1. Passive Attack

In passive attacks, an entrant the data changed while not sterilization it. The assailant doesn't actively initiate malicious actions to cheat different hosts. The goal of the assailant is to get data that's being transmitted, so violating the message confidentiality. Since the activity of the network isn't non- continuous, these attackers are tough to observe.

2. Active Attack:

In active attacks, an assailant actively participates in disrupting the conventional operation of the network services. A malicious host will produce a full of life attack by modifying packets or by introducing false data within the unintentional network. It confuses routing procedures and degrades network performance. Active attacks will be divided into internal and external attacks.

3. External Attack

External Attacks are carried by nodes that aren't legitimate a part of the network. In external attacks, it's doable to disrupt the communication of a corporation from the automobile parking space ahead of the corporate workplace.

4. Internal Attack

Internal Attacks ar from compromised nodes that were once legitimates a part of the network. In unintentional wireless network as approved nodes, they're rather more severe and tough to observe compared to external attacks. The most of the attackers [6] [7] ar moving the unintentional network performance and execute malicious activities at the time of causation and receiving the info. The attackers ar classified per totally different layer of network like Eavesdropping, jam assailant, blackhole attack, grayhole attack, byzantine attack [8], wormhole attack.

5. Attacks using Modification

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can set the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack is launch by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

6. Attacks using Impersonation

By impersonating a node (spoofing), a malicious node can cause many attacks in WSN . For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.

7. Attacks using Fabrication

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks is worm hole attack.
To make AODV secure, we need to understand security attributes and mechanisms. Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [5].

As WSN s use an open medium, all nodes can access data within the communication range. Therefore,

Confidentiality should be obtained by preventing the unauthorized nodes to access data.

Authentication should be used to ensure the identity of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes.

Integrity helps to prevent malicious nodes from altering data and resending it (called replay attack e.g. wormhole attack). Also, if a node sends a message, that node cannot

deny that the message was sent by it which is called **non repudiation [9].**
To defend against passive attacks conventional approaches like digital signature, encryption, authentication and access control (whether a node having appropriate access rights to access the network) should be considered. To defend against active attacks intrusion detection systems and cooperation enforcement mechanisms (reducing selfish behavior of a node) are useful.

III. CLASSIFICATION OF WORMHOLE ATTACK

It's troublesome to discover such dangerous attacks and nobody will predict what the hole nodes will do and wherever and once. The whole attack is invisible at the upper layer and so, two finish points of the hole aren't visible within the route during which detection becomes way more advanced. Hole is classified into additional four classes

- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

1. Open wormhole attack
In this attack malicious node keep examine the wireless medium to method the discovering RREQ packets, within the presence of malicious node within the network alternative node on the network suppose that malicious node square measure contribution on path and that they square measure their direct neighbors.

2. Closed wormhole attack
The assailant doesn't modify the capture packet nor did it modify the packet field head. The assailants take the advantage once the packets square measure within the method to search out a route apprehend as route discovery. At route discovery method attack tunnel the packet from one facet of the network to a different facet of the network and re-broadcast packets.

3. Half open wormhole attack
In this attack just one facet of the packet is modify from the malicious node and therefore the alternative facet of the malicious node don't modify the packet later on route discovery procedure.

4. Wormhole with high power transmission
In this attack malicious node use most level of energy transmission to broadcast a packet, once malicious node received a Route Request (RREQ) by exploitation route discovery method, it broadcast the Route Request (RREQ) at a most level of energy of it power therefore the alternative node on the network that square measure on the conventional power transmission and lack of high power capability hears the most energy power broadcast they beam the packet towards the destination.

IV. PREVIOUS WORK IN FIELD OF ATTACK

We can classify the attacks into two brief categories, namely passive and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation. There are some researchers are doing a work on attacks mentioned in this section.
In [10], a new security algorithm is proposed. In this scheme proposed algorithm consists of two phases. First is Suspicious Phase Source node A measures RTT from A to all of its immediate neighbors. Suppose B is one of the neighbors of A and if RTT between node A to node B is much higher than average value of RTT of all the links from A to its neighbors, then there is a possibility that both nodes A and B are no real neighbors but connected through tunnel and the node will be added into suspicious list. In Second Confirmation Phase all suspicious nodes, second phase is executed, that is confirmation phase. The node A as trusted neighbors calculates the shortest path to the suspicious node B. This shortest path does not include node As one hop neighbors.

In [11], a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high
Hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier.

In [12], wormholes are detected by considering the fact that wormhole attacks consists of relatively longer packet latency than the normal wireless propagation latency on a single hop. Since the route through wormhole seems to be shorter, many other multi-hop routes are also channeled to the wormhole leading to longer queuing delays in wormhole. The links with delays are considered to be suspicious links, since the delay may also occur due to congestion and intra-nodal processing.

In reference [13], both the hop count and delay per hop indication (DelPHI) are monitored for wormhole detection. The fundamental assumption in [13] is once again that the delay a packet experiences under normal circumstances for propagating one hop will become very high under wormhole attack as the actual path between the nodes is longer than the advertised path.

In this paper [15] proposed recent research work in field of wormhole attack is presents here and the security or detection scheme is provided some new idea of proposal against wormhole attacker. neighbors of sender and if RTT between sender to neighbor is much higher than average value of RTT of all the links from sender to its neighbors, then there is a possibility that both nodes A and B are not real neighbors but connected through tunnel and the node will be added into suspicious list. For all suspicious nodes, second phase is executed, that is confirmation phase.

In this paper [15], we propose a trust aware distance vector routing protocol (T-AODV) to protect wireless sensor network from wormhole attacks. To detect and prevent the network from these wormhole attacks, we propose an enhance version of AODV hello packets. The study assumes some assumption to apply our propose method such as the clock time is synchronized and used during neighbor discovery. Neighbor nodes respond with appending Hello massage with present received time and reply.

In this research [16] we analyzed the wormhole attack with four different scenarios with respect to the performance parameters of end to end delay, throughput, traffic received, utilization and network load. In a network it is important for a protocol to be effective and efficient in term of security. The finding shows that OLSR and AODV have more severe effects of wormhole when there is a higher number of nodes and more route requests.

V. PROPOSED WORK

In this paper, an efficient security scheme of to detect and prevention from wormhole attack called nearest neighbor based wormhole detection with AODV protocol has been proposed. In our proposed wormhole attack detection and prevention divided into two modules

- Detection module
- Prevention module

1. Detection Module

In this module we create data set of normal communication data profile and pass the generate output to detection module, if data match that means no deviation of data else data are modified or corrupted, after the identification of mismatch data we find out the reason of data dropping or modification, if we get data incoming in w1 node and forward to w2 node and drop the data into w2 node that link is a suspicious link and set as wormhole link in between w1 to w2 and also both node as a wormhole attacker node.

2. Prevention module

Preventer node watch the all neighbour node and if they found node receives the data but not forward to particular receiver of next hop than that preventer node indentified their address and previous node whose send data to attacker node address so both node treat as a attacker node because w1 and w2 node work in collaborative manner (w1 data receives and inform all the sender to re-initiation of route discovery process whose new fresh route not contain and wormhole node and protect the data from attacker.

Input:

S: set of sensor nodes
W1, W2: wormhole suspicious nodes Q_i: suspicious path
l_g: set of neighbour nodes T:
transmitter node
R: Receiver node
I: set of intermediate nodes
AODV: routing Protocol
CWP: Collaborative wormhole prevention Ψ: 550m^2 range

Output:

PDR, Throughput, delay, Attack Percentage, receives and sends information

Procedure:

T← execute-AODV (T,R,AODV)

While (S in ψ of T) **do**
I ← receive routing packets

I← forward (T,R,AODV) to next hop

If (T, R, AODV) receives by R **then**
R generate reverse path to T Send Ack to T node

Call data-pkt()

Else

R not in range

End if
End do

End if End do
Data-pkt(T,R,pkt) Count =1
If path is available then
All node in path set Q

lg watch I node
While pkt incoming I && forward I1 do
Check R receives those data or Not
If R != receives && pkt-forward ≠ true by I1 then
lg execute CWP in I and I1 node

If I forward data to I1 not forward to R then

I and I_1 set as w_1 and w_2 node by l_g(CWP)
l_g decide collaboratively to block w_1 and w_2
Roadcast blocking message in network

execute AODV by T
find new path which not include w_1 and w_2 node
End if Else
R receives partial data without attacker participation
R successful receives data by established path
End if
Calculate PDR = (receive/send)*100
packet_duration = end - start;

if
packet_duration > 0 **then** sum += packet_duration; recvnum++;
Calculate delay =sum/recvnum; Attack% = (100-(msends/tsend)*100); **End if**

The effect of proposed security scheme is visualized in results. The results are shows that the routing performance is almost equal as compare to normal AODV routing performance. The proposed scheme is identified the information of every neighbored and confirm the data delivery from every hop in network.

VI. RESULT ANALYSIS

Simulation results are evaluated on the basis of performance parameters like overhead, throughput etc. The simulation results are measured in case of normal AODV, Wormhole Attack, Previous IPS and Proposed IPS routing in MANET.

1. Simulation Paramters

The simulation of normal AODV, Wormhole attack and IPS scheme are done the basis of following simulation parameters that has shown in table1. These simulation parameters are decided on the basis of dynamic topology. In case of normal routing the node density scenarios of 30, 40and 50 nodes are consider for simulation.

Table I: Simulation Parameters.

Parameters	Value
Simulation Area	1000*1000
Network Type	WSN
Nodes/Devices	30,40.50
Physical Medium	Wireless
Node Movement	Random
Simulation Iteration	500
MAC Layer	802.11
Routing Protocol	AODV, IPS, Proposed IPS
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground
Rate	Random

2. Throughput Analysis

Throughput in measured to evaluated the packets receiving in per unit of time in network This graph are measured throughput in case of normal AODV, Wormhole Attack, Previous IPS and Proposed IPS routing. The throughput in presence of wormhole attack is negligible from start to end of simulation. The performance of Propose IPS is about 85% at the end of simulation and it is also higher about 90%. The proposed security scheme is provides the better performance in presence of attacker and completely block the misbehavior activity of wormhole attacker.

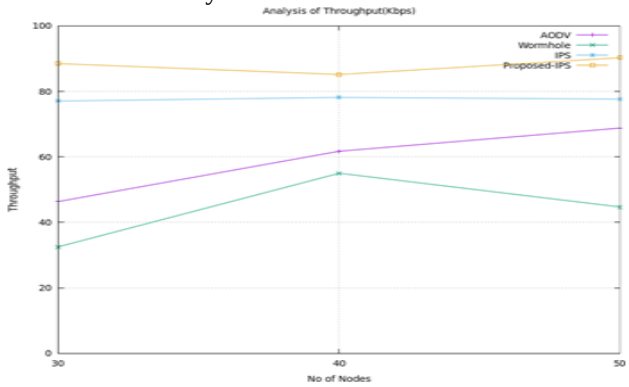

Fig.1. Throughput Analysis.

3. Delay Analysis

The Delay represents the number of packets are drop by attacker by that the receiver is not received the packet in network w.r.t time. This graph is measured delay performance in case of normal AODV, Wormhole Attack, Previous IPS and Proposed IPS routing. The packets dropping is minimized because the complete packets are drop by attacker. But in Proposed IPS packet dropping is zero and not a single packet is affected by wormhole attack. Proposed IPS will block the whole activity of wormhole attack and remove the infection from network that reduces delay in the network.

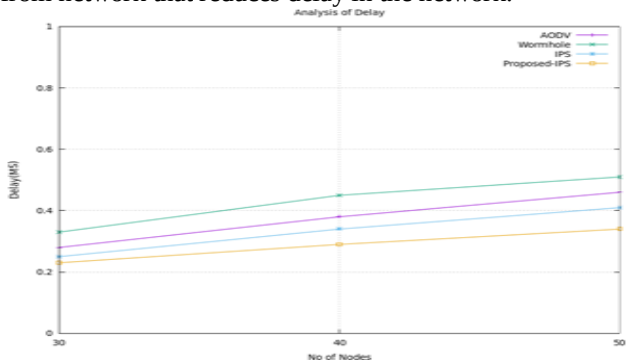

Fig.2. Delay Analysis.

4. NRL Analysis

The routing packets are important to know the information about the receiver. This graph is measured delay performance in case of normal AODV, Wormhole Attack, Previous IPS and Proposed IPS routing. The NRL oin presence of attack is high almost about 0.6. The routing packets are deliver in network in Proposed IPS overhead is about 0.4 in 50 node density scenario. The important point of normal routing is the minimum value of routing packets are show the better performance in network and this performance is determine in case of

attack and the important point is that in minimum routing packets the actual data packets are deliver in network are less in quantity as compare to normal and IPS routing. In case IPS the routing packets are more deliver because of identifying the secure path for communication.

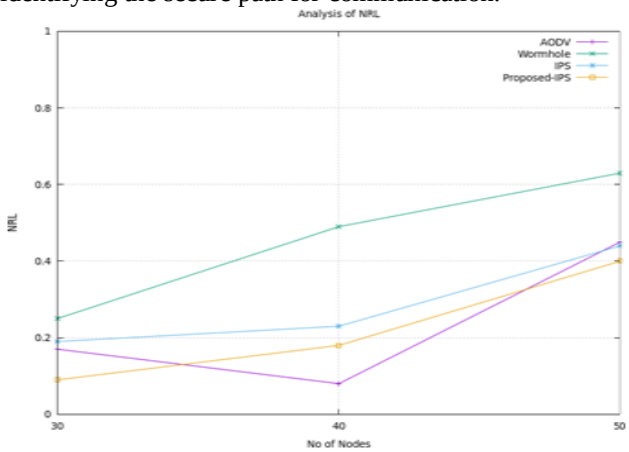

Fig.3. NRL Analysis

5. Data Sending Analysis

The number of packets sends in network is measured in case of normal AODV, Wormhole Attack, Previous IPS and Proposed IPS routing. The proposed scheme improves packets sending and provides the better performance in presence of attacker. The numbers of packets are delivering in time limit that's why unnecessary delay in network is also controlled. The packets sending in case of wormhole attack is very less. The packets sending in case of Propose IPS is nearby 40000 packets up to the end of simulation in all node density scenarios. That is more as compare to wormhole attacker.

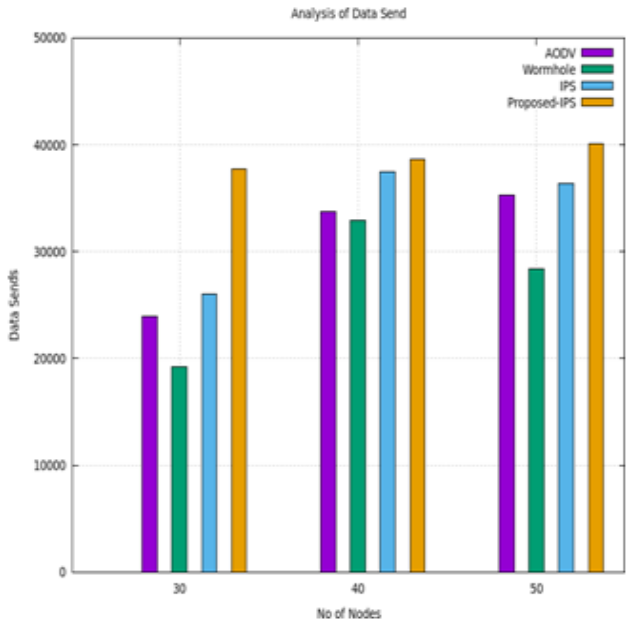

Fig.4.Data Sending Analysis.

6. Data Receiving Analysis

This graph is measured packets receiving analysis in case of normal AODV, Wormhole Attack, Previous IPS and Proposed IPS routing. The proposed scheme improves packets receiving and provides the better performance in presence of attacker. The packets receiving in case of wormhole attack is very less. The packets receiving in case of Propose IPS is nearby 37000 packets up to the end of simulation in all node density scenarios. That is about 2 times more as compare to wormhole attacker.

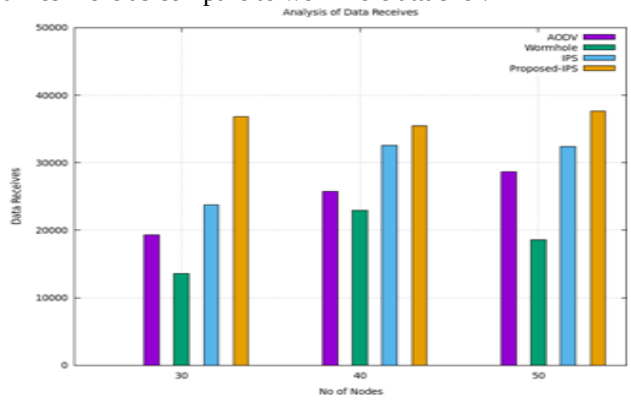

Fig.5. Data Receiving Analysis.

7. Packet Delivery Ratio

The PDF performance is evaluated the percentage of data per unit of time received at destination. The PDF performance in case of normal AODV routing, Wormhole Attack, Previous IPS and Proposed IPS routing. is mentioned in this figure. Here the network performance in presence of wormhole attacker is negligible, that shows the zero packets receiving at destination but in presence of proposed IPS the attacker activity is completely blocked through broadcasting the attacker identification (ADI). The proposed security scheme is provides the normal performance as nearly equal to normal AODV and improves the network performance in presence of wormhole attacker.

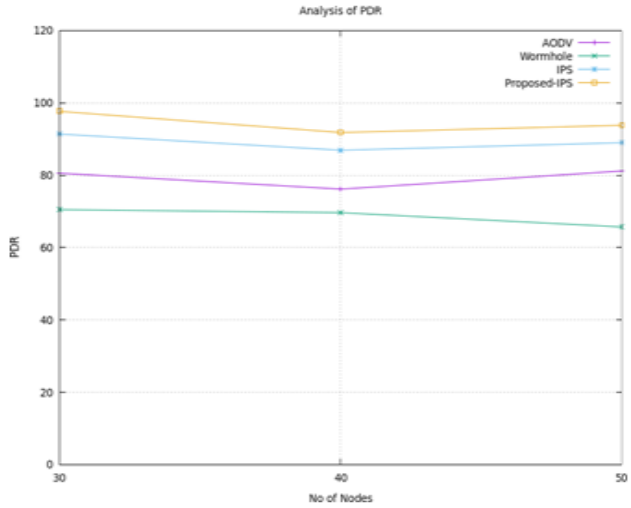

Fig.6. PDR Analysis.

VII. CONCLUSION AND FUTURE WORK

A WSN is built, operated, and maintained by its constituent wireless nodes. These nodes generally have a limited transmission range and so each node seeks the assistance of its neighboring nodes in forwarding packets. Wireless Sensor Network (WSN) has emerged as a new frontier of technology to provide anywhere, anytime communication. Due to its deployment nature, WSN is more vulnerable to malicious attack The Proposed prevention scheme against wormhole attack are protect data capturing through mis-activity, in this scheme we apply profile base detection and route trust base prevention technique, for securing data communication. very first we generate normal activity profile and compare with new generated profile if not match that means our new arrival data is unsecure data and we get particular attacker node and if we found the attacker node than we apply route IPS mechanism and block the attacker node and prevent the our network communication against wormhole attack.

The previous work is provides the idea about how the different security scheme is apply the proper procedure to secure WSN routing performance. Significant performance parameters such as infection rate throughput, delay, node density and packet delivery ratio. The study focuses on how performance of network affected under wormhole attack in a network and result comparison is shows that the performance of proposed scheme is provides the better results as compare to previous scheme. In future we also examine the behavior of other attacks like Advanced Persistent Threat (APT) attack and try to make the protection schemes on it and also try to enhance the performance of routing protocol that has consider in this dissertation to improves their routing capability.

REFERENCES

[1]. C.Siva Ram Murthy and B S Manoj, 'Wireless Sensor Networks-Architecture and Protocols", Pearson Education, ISBN 81-317-0688-5 ,2004.

[2]. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Sensor Networks Technologies and Protocols, Springer, 2005.

[3]. S. Choi, D. Kim, D. Lee, J. Jung. "WAP: Wormhole Attack Prevention Algorithm in Wireless Sensor Networks". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.

[4]. Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan and Barber Aslam,"Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16, pp. 29-33, 2006.

[5]. Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research, pp. 430-443, 2009.

[6]. Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof.
J.S. Deshpande, " A Survey of Wireless Sensor Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[7]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Wireless Sensor Network ,"Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 1-38, @ 2006 Springer.

[8]. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[9]. 6Khin Sandar Win," Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008.

[10]. Mousam A. Patel, SRPEC, Unjha, Manish M. Patel, "Wormhole Attack Detection in Wireless Sensor Network", Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA), 2018.

[11]. Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo. "A Hop- Count Analysis Scheme for Avoiding Wormhole Attacks in WSN ", 9 (6), pp. 5022-5039, 2009.

[12]. F. Nait-Abdesselam, B. Bensaou, T. Taleb. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communications Magazine, 46 (4), pp. 127 - 133, 2008.

[13]. H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.

[14]. Mousam A. Patel, Manish M. Patel "Wormhole Attack Detection in Wireless Sensor Network" Proceedings of the International Conference on Inventive Research in Computing Applications, (ICIRCA), pp.269-274,2018.

[15]. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks", IEEE International Conference on Smart Sensors and Application (ICSSA), 2015.

[16]. Mohammad Sadeghi and Dr Saadiah Yahya, "Analysis of Wormhole Attack on WSN s Using Different WSN Routing Protocols", IEEE Fourth International Conference on Ubiquitous and Future Networks (ICUFN), pp.301-305, 2012.