Detection and Prevention of Wormhole attack Over Wireless Ad-Hoc Network

Rahul Malviya[1], Mr Amit Thakur[2]
Research Scholar[1], Head of Department[2]
Swami Vivekananda College of Science & Technology, Bhopal
rahul.malviya420@gmail.com[1]

Abstract**—** Sensor network is infrastructure-less network in which communication takes place between mobile nodes, packet is transmitted with the help of intermediate nodes. Nodes are capable of moving free in the network, they can leave or join the network when it is needed. Hence with the dynamic changing nature sensor network is vulnerable to various security attacks. These attacks hinder the network performance. Sensor network, security is considered as one of the critical issue. In this paper we concentrate on the noxious conduct of AODV under wormhole attack. In our propose work we make zones on the basis of node range and at whatever point we produce Rreq we send previous information. On the premise of previous information check and zone data we identify wormhole and for counteractive action we stream normal way node_id in the system.

Keywords**—**Sensor Network, Wormhole attack, Security, AODV

I. INTRODUCTION

Sensor Network is a collection of mobile nodes that communicate among each other with the help of intermediate nodes. It is an infrastructure-less network hence prone to various types of attacks. Security is one of the major factors that degrade the performance of Sensor Network. Sensor Network characteristics and key challenges are presented in [1].

a. ADVANTAGES OF SENSOR NETWORK

The advantages of Sensor Network include the following:

- **i.** Access to information and services regardless of location and position.
- **ii.** Provides scalability
- **iii.** Improved Flexibility.
- **iv.** Robust due to decentralize administration.
- **v.** Simple fast and cheap setup of network.

b. SECURITY ATTACK

Attack is an attempt to destroy or interrupt the normal functionality of the network and violate the basic security goals which are as: confidentiality, authentication, integrity, availability and non-repudiation. Various security issues are present in Sensor Network [2]. Attacks are of two types depicted in the fig1: passive attack and active attacks.

- **i. Passive attack:** Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Passive attack violates confidentiality.

- **ii. Active attack:** Active attacks are very severe attacks on the network that prevent message flow between the nodes These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. Active attack violates integrity. Active attacks are present in the network at different layers. Different types of attacks have been explained in figure 1.

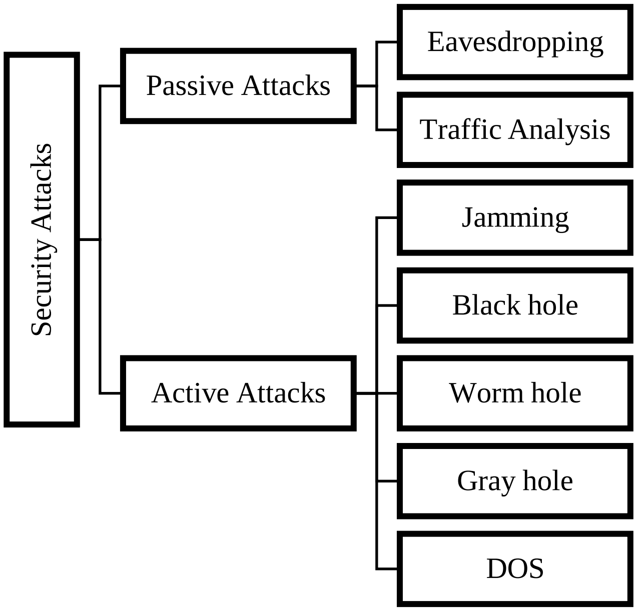

Figure 1: Hiearchy of Security Attak Over Sensor Network

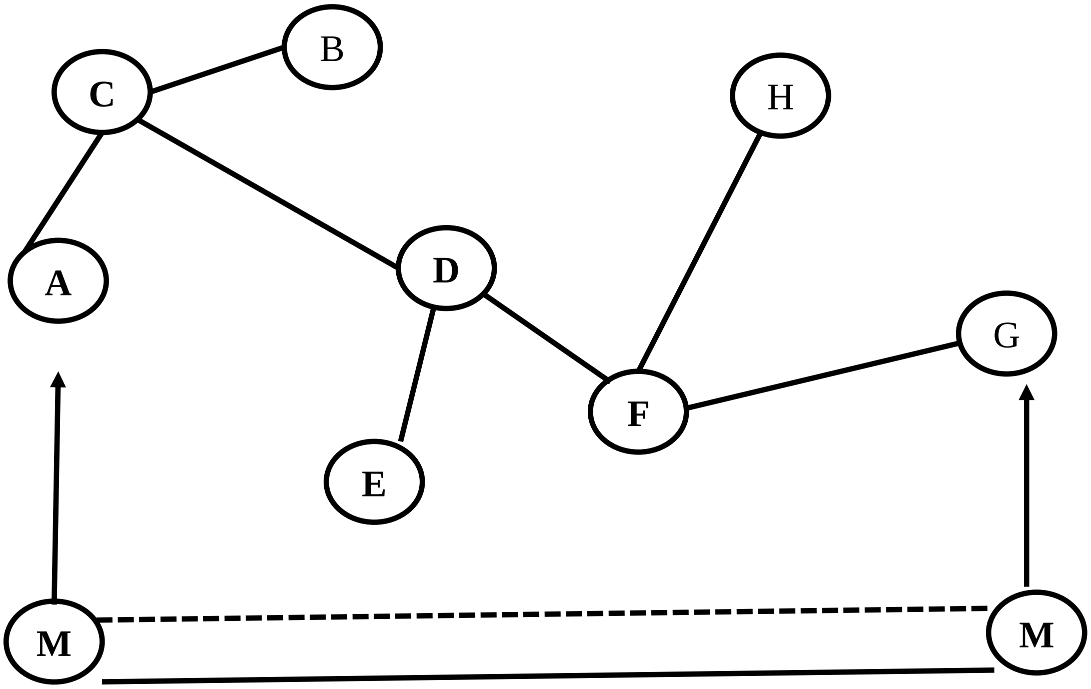

Figure 2: Wormhole Attack

II. ROUTING PROTOCOL

Ad-Hoc network routing protocols are mainly classified into following classes; Proactive, reactive and hybrid protocols [3].

i. **Proactive protocol**: It is also known as table-driven routing. Firstly route has to be determined and all nodes maintains the routing information about other nodes residing in the network and routing updates are broadcasted in the network whenever network topology changes. DSDV, CGSR, OLSR are proactive protocols.

ii. **Reactive protocols:** These are on demand routing protocols, a node only knows the routes it actually requires, find a route (route discovery) only when node wants to send data to a node. Maintains the route (route maintenances) only active routes are maintained.AODV, DSR are reactive protocols.

iii. **Hybrid protocols:** It is a Combination of both proactive and reactive routing protocols. ZRP is hybrid protocol.

a. AODV Routing Protocol

The AODV [4] routing protocol is an on demand routing protocol. Whenever there is need of path between source and destination then the route establishment is done. Once the route is established it remains till the time it is needed. Route discovery procedure is initiated to find the valid path between source and destination if any valid path is not available in the table. After route is established the data packet is forwarded to destination, only active paths are maintained in the table.

III. WORMHOLE ATTACK

Wormhole attack [5] is such type attack which comprises of two nodes known as the attacker nodes linked to one other via tunnel. The attacker node that resides at one side in the network occupies the packet from the authentic node and encapsulates the packet and with the help of tunnel transmits it to the other attacker node or malicious node present in the network. It consists of one or two malicious nodes and a tunnel between them. Wormhole nodes forge a route that is shorter than the actual path within the network means it create mirage for the legitimate node so that they believe the route is shorter than the actual one. However it is not compulsory that the route by the wormhole nodes might be shorter. Fig 2 represents example of wormhole [5].

In given fig 2, here we have two malicious nodes M1 and M2 connected with each other with the aid of a link, known as tunnel, “the wormhole tunnel” by which malicious nodes transmits the packet to one other as well as the entire traffic follow this route via tunnel.In the fig 2, node A and node G are represented as source and destination respectively. So now the source node A will forward the packet to the legitimate neighbor i.e.; node C in this way intermediate nodes between node A and node G i.e., C, D, F will forward the packet from source to destination. In the absence of malicious nodes the legitimate path from node A to node G will be A-C-D-F-G so number of hops the packet travels is 3(three). Now when wormhole nodes are present as well as they are malicious nodes so now the nodes M1 and M2 will get activated making an illusion to source and destination of being immediate neighbors, capable of hearing one's request so transmission take place among node A and node G via node M1 and node M2.

A: Types of Wormhole attack

Different types of wormhole attack are described in different literatures [5, 6].

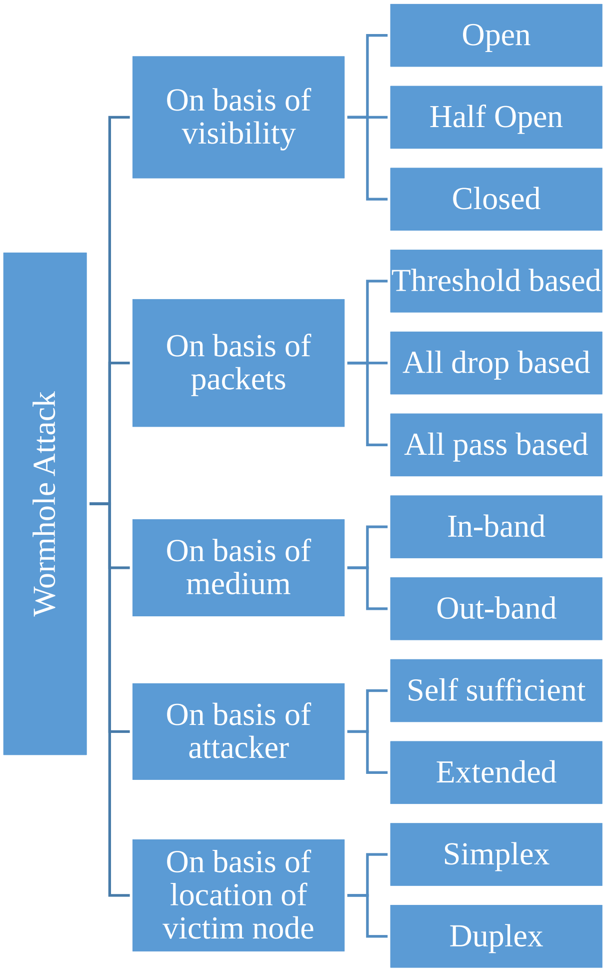

Figure 3: Hierarchy of wormhole attack

a. MODES OF WORMHOLE ATTACK

The given figure 2 depicts the various modes of operations of wormhole attack. With the help of these modes wormhole attack is launched [2].

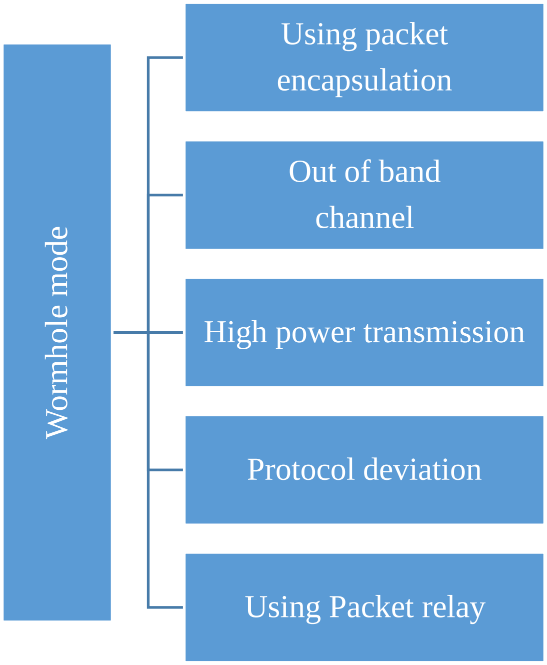

Figure .4 Modes of wormhole attack

IV. RELATED WORK

Biswas et al [7], this method is an enhancement to the existing "WAP" technique. The new proposed method is capable of detecting the false positive alarm known as WADP, (wormhole attack detection and prevention.). It provides the two way verification by collaborating WADP with node authentication in modified AODV. It is able of detecting both the hidden as well as exposed attack. Detection of hidden attack is done on basis of neighbor node list and timer.

Detecting exposed is done by calculating the delay per hop. In this way both attacks are detected. For detecting false alarm in the reply packet adding two new fields ip address of intermediate node and a unique number. By this combination malicious nodes are detected and isolated from the network and resolves the issue of false alarm. Below are described the problems related to this approach.

V. PROBLEM STATEMENT

1. Each node maintains the information of its neighbor node in a routing table. A node monitors the behavior of its neighbours. Information related to path is also stored. This is time consuming and increases the overhead on nodes.
2. A node can be treated as a malicious node. When radius of a node is small and node is mobile moves out of the transmission range of the other nodes for particular time duration and when it returns in the network that time the node can be treated as wormhole node.

3. Packet can be modified. As for node authentication in the RREP packet two fields the IP address as well as unique number are used. When a node forwards a RREP packet toits neighbor node it verifies the combination as theauthentic node knows this information. When passive attackis launched it cannot detect it as a result packet can be modified as the nodes are unable to collect the correct information.
4. When any node forward a RREQ packet to its neighboring node it records the sending time of the packet and when the node overhears the RREQ packet after the set time the node which sends the RREQ packet is considered as a wormhole node.

VI. Proposed Work

In our propose work presenting a scheme named as path routing zone. In path routing zone we create zones on the basis of node range and whenever we generate RREQ we send previous path information. Depending on the previous path check as well as zone information we detect wormhole and for prevention when a source node transmits the request packet to its first neighbor node, the neighbor node forward the packet to its neighboring node the suspicious node i.e. at one hop distance from it.

The malicious node transmits the request packet with the help of tunnel to other malicious node. The second malicious node either forwards the request packet to destination or discards the packet or drop the packet. So the source node creates a path routing zone with the nodes its first neighbor node, including both the malicious nodes.

Path routing zone detects the malicious nodes. After forwarding the packet the source node waits for the ack packet (acknowledgement packet), when the ackpacket is not received by the source node it sends the RREQ along with the previous path information to its other neighboring node excluding the first neighbor node.

Neighboring nodes generates a RREP packet and send the node_id and the distance between nodes. Source node asks its other neighboring nodes about the previous path zone that was created by the source to verify that all the data if passes to these malicious nodes that pretends to be the shortest path to destination, then these nodes are treated as suspicious nodes. Notes the communication that takes place between these nodes and then blacklist the malicious nodes. By placing the malicious nodes in blacklist we are avoiding the wormhole nodes.

Proposed Algorithm:

```
Step 1: set up the network.
Step 2: on the basis of node range create zones.
Step 3: flood the RREQ packet in the network.
Step 4: follow the shortest path.
Step 5: if not receiving acknowledgement Threshold>2
        {
           Goto step (6)
        }
    Else
        Follow the path
Step 6: Then generate RREQ, for new path.
Step 7: Send new RREQ packet which contains: RREQ+ previous path info to neighbor node.
Step 8: Nodes generate a RREP and send the node_id with the distance of neighbor nodes.
Step 9: if (prev path info == new path info)
        Then Goto step (10)
        Else
          Follow the path. Store the values in routing table.
Step 10: check the distance between the nodes.

Step 11: if the distance of few nodes is always same for
        all RREQ or the next hop is same then check the
        reception of acknowledgement for that node.
        Else
        Node is legitimate and follows the path
Step 12. If acknowledgement received the node is legitimate node. Follow the path
        Else
           The nodes is wormhole. And blacklist these nodes.

Step 13: finish
```

VII. Simulation Results

The simulation is carried over ns-2. The total number of nodes is 14. The X-Y dimension is 800X800. The routing protocol used is AODV.

Table.1 Simulation Parameters

Parameters	Value
Channel	Wireless
Propagation	Two Ray Ground
Network Interface Type	Wireless Physical
MAC type	Drop tail
Link Type	Logical Link
Queue length	50
Number of nodes	14
XY dimension	800X800
Routing Protocol	AODV
Simulation ends	100.0ms

A: **Packet Delivery Ratio:**

By packet delivery ratio we mean that, the ratio of total number of packets delivered from source to destination. It is a fraction of total number of packets delivered by total number of packets send.

The minimum value of packet delivery ratio of existing approach is 114 in 10miliseconds and maximum is 150 in 40 ms, when running the scenario of proposed approach the minimum value is 119 at 100ms and maximum is 149 in 40ms. The overall ratio of packet delivery of proposed approach is good.

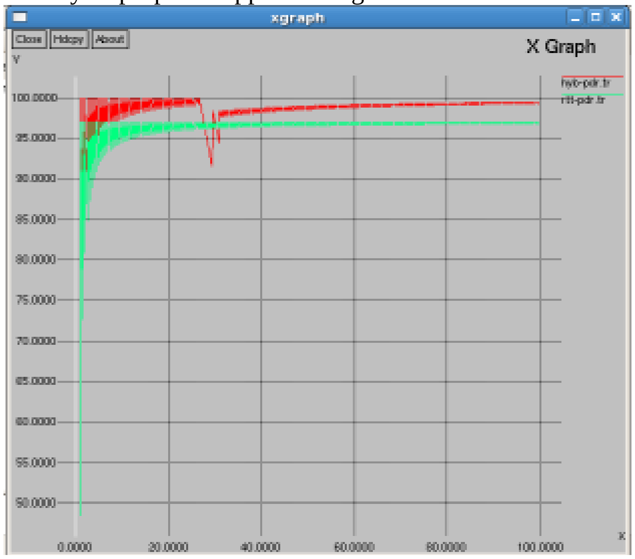

Figure 5: Packet Delivery Ratio

Routing packet overhead: - For any ideal routing protocol it is required that it has lower routing packet overhead, whereas existing approach by using Hop Based On Potential Field have required higher routing packet as compare to proposed methodology by using rtt based hop.

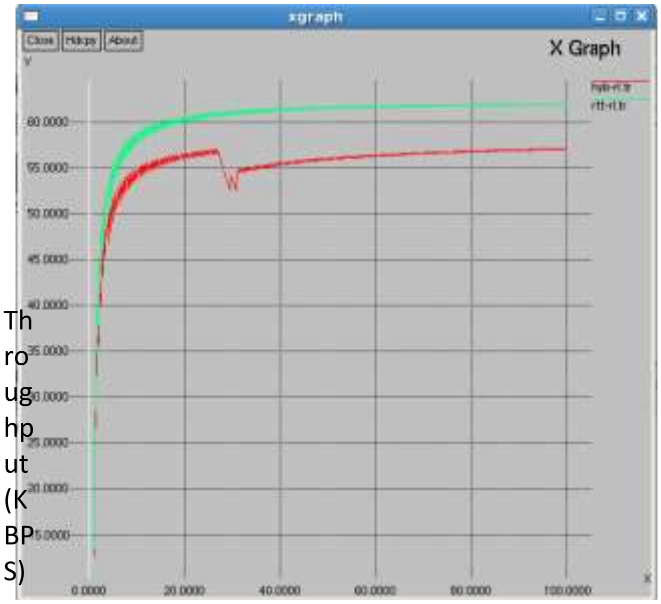

Figure 6: Routing Overhead

Battery Power Consumption:-Towards Energy saving routing protocol proposed protocol try to move lower energy node towards less traffic and higher energy node towards high traffic and reduce retransmission whereas existing approach only minimized redundant path. Existing approach by using RTT Based required higher battery power consumption as compare to hybrid approach by using rtt and hop based. Figure 7 shown remaining energy that means higher remaining energy means lower energy consumption.

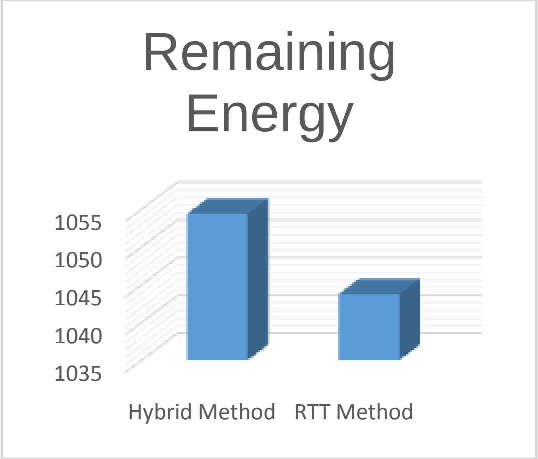

Figure 7: Remaining Energy

Throughput: - In any sensor network it is required to have higher throughput ie need to increase rate of successful packet transmission. Average data rate of successful data or message delivery over a specific communications link. Network throughput is measured in bits per second

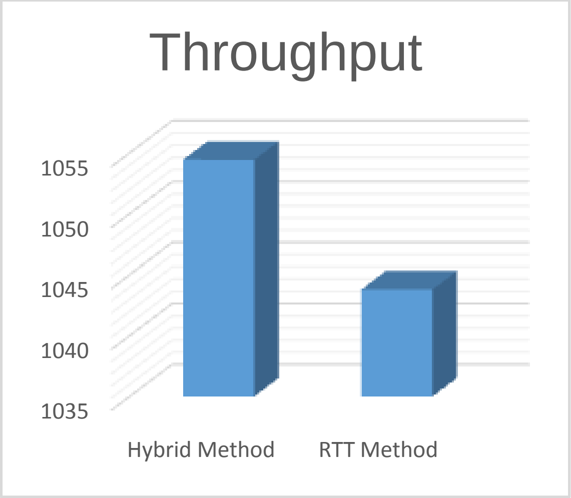

Figure 8: Throughput

VIII. CONCLUSION

In this paper, presenting a zone based path routing approach for detecting as well as preventing wormhole attack in Sensor Network. Wormhole attack severely degrades network performances. Finding out this attack in network is difficult. The existing approach when applied on network does not provides better outcomes whereas when applying proposed approach it provides improved results in terms of packet delivery ratio, send packets, received packets and drop packets. In future, we will apply optimization technique for better results.

REFERENCE

[1] N. Marchang, R. Datta and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1684-1695, Feb. 2017.

[2] Y. Zhang, L. Wang, W. Sun, R. C. Green and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," 2014 IEEE Power and Energy Society General Meeting, San Diego, CA, 2014, pp. 1-8

[3] T. S. Bharati and R. Kumar, "Secure intrusion detection system for mobile adhoc networks," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 1257-1261.

[4] G. Indirani and K. Selvakumar. 2014. A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks MANET. Int. J. Parallel Emerg. Distrib. Syst. 29, 1 (January 2014), 90-103.

[5] S. Sumit, D. Mitra and D. Gupta, "Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining," 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), Faridabad, 2014, pp. 156-160.

[6] Dahai Du and HuagangXiong, "A dynamic key management scheme for Sensor Network," Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, Harbin, 2011, pp. 779-783.

[7] A Kumar, K. Gopal and A. Aggarwal, "A complete, efficient and lightweight cryptography solution for resource contrainst Mobile Ad-Hoc Networks," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, 2012, pp. 854-860.

[8] S. Balfe, K. D. Boklan, Z. Klagsbrun and K. G. Paterson, "Key Refreshing in Identity-Based Cryptography and its Applications in Sensor Network," MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, 2007, pp. 1-8.

[9] ZunnunNarmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[10] Sheikh, R. , Singh Chande, M. and Mishra, D.K., “Security issues in MANET: A review”, IEEE 2010, pp 1-4.

[11] Anderson, J.P., Computer security threat monitoring and surveillance. 1980, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

[12] Sumit, S., D. Mitra, and D. Gupta. Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining. 2014. IEEE.

[13] Preetee K. Karmore ,Smita M. Nirkhi, Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining. International Journal of Computer Science and Information Technologies, 2011. 2(4): p. 1774-1779.

[14] Indirani, G. and K. Selvakumar, A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET). International Journal of Parallel, Emergent and Distributed Systems, 2014. 29(1): p. 90-103@ 1744-5760.

[15] Yogita B. Bhavsar , KalyaniC.Waghmare, Intrusion Detection System Using Data Mining Technique: Support Vector Machine. International Journal of Emerging Technology and Advanced Engineering, 2013. 3(3): p. 581-586.

[16] Panwar, S.S. and Y.P. Raiwani, Data Reduction Technique to analyze NSL-KDD set .Journal Impact Factor, 2014. 5(10): p.21-31

[17] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., “ A survey of routing attacks in mobile ad hoc networks” IEEE 2007, pp 85-91.

[18] Verma, M.K. and Joshi, S. ; Doohan, N.V. “A survey on: An analysis of secure routing of volatile nodes in MANET”, IEEE 2012, pp 1-3.

[19] P. Papadimitratos and Z. J. Haas, “Secure Routing For Mobile Ad Hoc Networks” in Proc. of CNDS, 2002.

[20] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, “A Secure Routing Protocol For Ad Hoc Networks” in Proc. of IEEE ICNP, 2002.

[21] C. E. Perkins, and E. M. Royer, “Ad-hoc on-demand distance vector routing,” IEEE 1999, pp 25-26.

[22] Mahdi Nouri, SomayehAbazariAghdam and SajjadAbazariAghdam, “Collaborative Techniques for Detecting Wormhole Attack in Sensor Network”, IEEE 2011, pp1-6.

[23] Ali Modirkhazeni, SaeedehAghamahmoodi, ArsalanModirkhazeni and NaghmehNiknejad, “Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks”, IEEE 2011, pp 122-128.

[24] Mariannne. A. Azer, “Wormhole Attacks Mitigation in Ad Hoc Networks”, IEEE 2011, pp 561-568.

[25] Jin Guo, Zhi-yong Lei, “A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification”, IEEE 2011, pp 564-568.