International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 155-160
Published Online August 2020 in IJEAST (http://www.ijeast.com)

SINKHOLE ATTACK DETECTION IN MANET USING SWARM INTELLIGENCE TECHNIQUES

Laxmi
J.C Bose University of Science and Technology
YMCA Faridabad, Haryana, India

Dr. Rashmi Popli
J.C Bose University of Science and Technology
YMCA Faridabad, Haryana, India

***Abstract*— Mobile Adhoc Network (MANET) is multi-hop remote system of self-governing versatile nodes with no preset framework where each node can move toward any path to play a task of router. In a mobile ad-hoc network (MANET), there is a short-lived network setup by unbounded nodes, which move anywhere and communicate within the absence of centralized network. Sinkhole attack may be a network layer attack, which affect the overall network. The information is attracted by sinkhole node from the neighboring node and after that, it counterfeits the steering data that makes the local area network know its way on specific node. Therefore, sinkhole tries that all the data passed through this node. Therefore, it modifies the packet information or drops the packet silently. This paper includes the optimization of route for sinkhole attack using Ant colony optimization and detects the sinkhole attack by using the Enhanced Particle swarm optimization technique. This paper also uses the MD5 (Message Digest) Algorithm for hashing and voting method for ranking the nodes.**

Keywords— **MANET, ACO, EPSO, MD5, RREQ, RREP**

I. INTRODUCTION

Mobile Adhoc Network (MANET) is a self-organizing system of movable mobile nodes joint by wireless connection without any entrance point. Each movable node is self-managing node and there is not any central node for managing the mobile network. The movable nodes have permission to shift anywhere according to its need. It allows that the nodes can easily join or leave the network. The capability of the nodes for communication is not limited. When the connection is established and the nodes lie outside from the radio range of network then it may cause loss of data.

Sinkhole attack is type of network layer attack and it represents the problem against routing protocols. A sinkhole node may alter or drop the packets in order to gain the packet information to itself. It sends the fake routing information to all the nodes that it has an optimum route to the destination so that all the network traffic can go through it. This malicious can drop or modify the packet to destroy the network. Sinkhole attack can execute other attacks like Selective forwarding attack, Jamming attack, and wormhole attack.

The architecture of MANET is shown in figure.1.

.

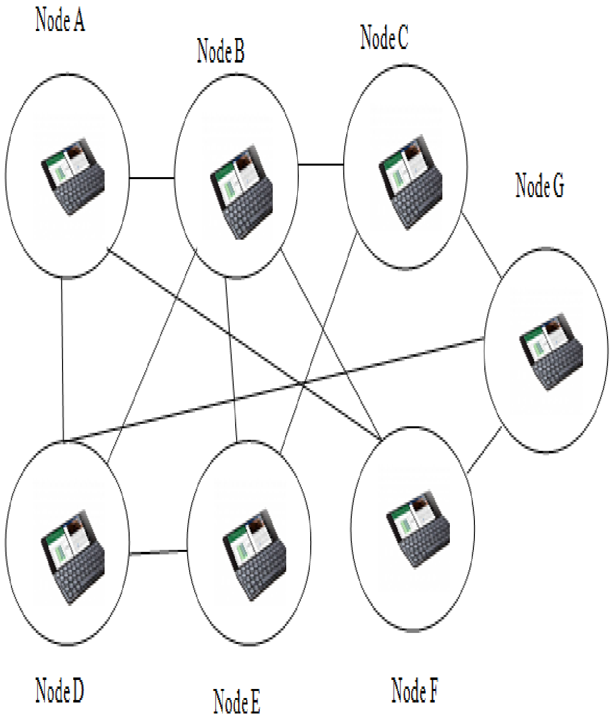


Fig 1: Mobile Adhoc Network

The main focus of this research is to propose a sinkhole attack detection technique. In this paper, we proposed an effective sinkhole attack detection technique. The sinkhole detection algorithm composed of two main techniques namely Ant Colony Optimization (ACO) and Enhanced Particle Swarm optimization (EPSO). Ant Colony Optimization technique is used for path Optimization and Enhanced Particle Swarm Optimization technique is used for sinkhole detection. The rest of this paper is organized as follows. In Section 2, we describe the sinkhole attack. In section 3, the related work about the detection of sinkhole attack using various approaches are presented. In section 4, the proposed sinkhole detection method is presented. In section 5, the simulation techniques used in detection are described. In Section 6, simulation results to evaluate the proposed method are presented, and we make concluding remarks in Section7.

II. SINKHOLE ATTACK

Sinkhole attack is one of the intrusion attacks in MANET. In this attack, an attacker sends the fake routing information and insists that it has an optimum route to the destination for the data transmission. Then most of the nodes pass the data packet through this malicious node and it results in dropping off data packets.

In a sinkhole attack, an interloper bargains a node or presents a fake node inside the network and utilizes it to cast an attack. The sinkhole node tries to attract all the data traffic from its neighbour node based on the routing buffer used in the routing protocol[3]. A sinkhole attack prevents the base station from achieving complete and correct sensing data and it is harmful to upper layers. Sinkhole attack is difficult to beat. Routing information supplied by a node is crucial to verify. By using this sinkhole attack, data packets can be dropped and information can be altered. It may cause disorder in the network. In sinkhole attack the malicious node can easily join the network, modify the information or may drop the packets and after that, it leave the network without being detected. The architecture of Sinkhole attack is shown in figure.1.

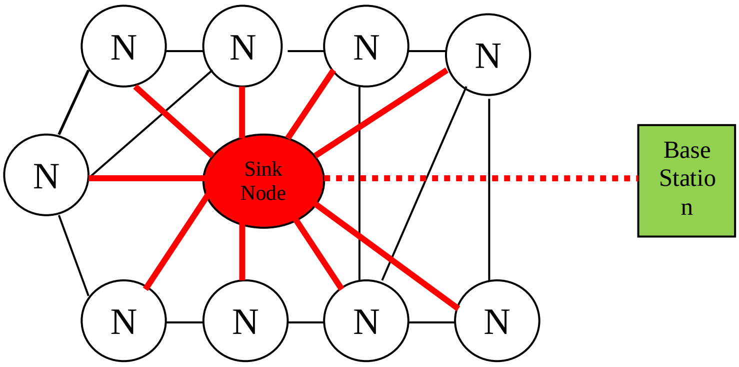


Fig 2: Sinkhole Attack

III. RELATED WORK

Sinkhole attack is major threats to mobile adhoc network. Sinkhole attack is a type of network layer attack where the malicious node sends the fake routing information to its closed nodes and claim that it has an optimum path from source to destination node. In sinkhole attack, it is not required to target all the nodes in the network only its closed nodes are enough to target.

It is recognized that some recent works in sinkhole attack detection in MANET use various techniques such as Particle Swarm Intelligence, Genetic Algorithm, Artificial Bee Colony Optimization, Ant colony Optimization and many more techniques. The various techniques are as follows:

Gisung Kim et. al. propose a model to detect sinkhole attack in MANET. This Sinkhole attack detection is considered with DSR (Dynamic Source Routing) protocol [10]. In this paper, a cooperative sinkhole attack detection method using analyzed features is presented. This algorithm uses three packets namely SAP (Sinkhole Alarm Packet), SDP (Sinkhole Detection Packet) and SNP (Sinkhole Node Packet)[5]. A sinkhole indicator is also used and when sinkhole indicator is detected, the attack detection algorithm is initiated by SAP. SDP and SNP both are used to detect sinkhole node. This model improves the performance in terms of detection rate and detection time.

Vikas Raina and Sulekha Kumari et. al. proposed an approach to detect sinkhole attack in MANET using Genetic Algorithm. This paper focuses on Optimization of packets and data route using weight function. In this, an AODV protocol is used to modify the network parameters. In this paper, the cluster head and number of rounds are must be specified[2]. If the sinkhole node is not found then it produces number of copies in the network to over the load in the network. It is conclude that Genetic Algorithm provides better performance in optimizing sinkhole attack.

Iqbal Singh and Harpreet Kaur et. al. propose a method to detect sinkhole attack Using OLSR routing protocol with Artificial Intelligence OLSR routing protocol is use for discovering route among source and destination. ABC (Artificial Bee Colony) is used with OLSR protocol[4]. In this research, ABC algorithm is used for optimization and the ANN (Artificial Neural Network) is used for classification. It reduces the BER (Bit Error Rate) or rate of energy consumption and increases the throughput rate[8].

N K Sreelaja et. al. proposed a technique to detect a sinkhole attack in WSN (Wireless Sensor Network). This technique finds a malicious node in WSN using ACO based approach. The ACO-AD Algorithm detects sinkhole attack effectively and does not generate false positive. The ACO-AD generates less number of searches as binary search and linear search.

G. Keerthana, G. Padmavathi, proposed detecting Enhanced Particle Swarm Optimization algorithm to detect Sinkhole Attack In WSN (Wireless Sensor Network). In this paper particle Swarm Optimization technique is used for detecting sinkhole attack [1]. In this paper Ant Colony Optimization Algorithm is used to detect Sinkhole attack. In this the three algorithms namely Ant Colony Optimization algorithm, Particle Swarm Optimization and Enhanced Particle Swarm Optimization are used and after that compares which technique gives best result for Sinkhole attack detection [1].

Shubh Lakshmi Agrwal et. al. proposed an algorithm for short route finding in sinkhole attack detection and prevention in MANET. This paper presents an individual trust managing technique to prevent against sinkhole attack. Whenever a RREQ packet is expended to one hop neighbour, sinkhole node alters the hop count from itself in RREQ packet. It creates an illusion of short route to the destination node. When RREP packet is generated, the updated hop count information is added to the RREP packet when source receive a RREP from malicious node it finds the short route by the sinkhole node. Therefore, it decreases the PDR (Packet Delivery Ratio).

Table 1: Comparison Of Sinkhole Attack Detection Method

AUTHORS	TECHNIQUES	TOOL	OBSERVATIONS	YEAR PUBLISH
Gisung Kim et. al.	Cooperative sinkhole detection method	NS2	Improves detection rate and detection time	2009
Vikas Raina et. al.	Genetic Algorithm and AODV Protocol	MAT-LAB	Increase Throughput and PDR, decrease Delay	2017
Iqbal Singh and Harpreet Kaur et. al.	Artificial Neural Network And Artificial Bee Colony	MAT-LAB	BER and Rate Of Energy is reduced and Throughput is increased	2018
N K Sreelaja et. al.	ACO-AD algorithm	MAT-LAB	Number of searches is less and does not generate false positive	2014
Tejindereep Singh et. al.	RREQ and RREP are used	NS2	Decrease packet loss and increase packet delivery	2013
Shubh Lakshmi Agrwal et. al.	AODV base routing algorithm	NS3	Increase PDR and decrease End to End delay is decreased	2016

IV. PROPOSED METHODOLOGY

This proposed methodology is divided into 3 parts:

- Route discovery process
- Route optimization process
- Sinkhole attack detection process

4.1 Route Discovery Process

In this process firstly the nodes environment is created with various nodes. Source node wants to establish the connection for transmitting the data to the destination node. Source node sends the data packet to the destination using some middle nodes. These middle nodes are called the Routers. If the source find the Route from source to destination node then it sends the data packet otherwise it sends the RREQ(Route Request) to the destination node for finding the data path. If route is Discovered then the destination node sends the RREP (Route Reply) message to the source node which contains the node ID, Sequence number and other details. If these details are matched with the source node details then connection is established otherwise connection is lost.

In figure 3, various routes are available from source to destination and we have to choose best route for the data transfer.

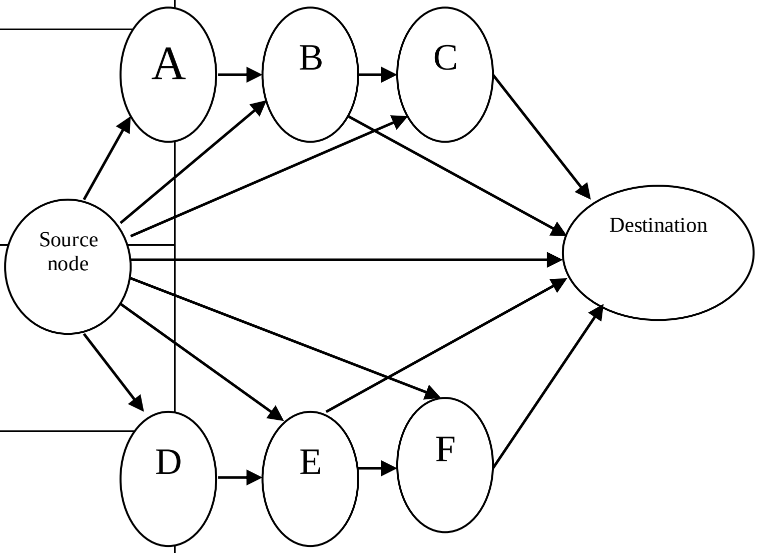


Fig3: Route Discovery

4.2 Route Optimization Process

In this section, the ACO (Ant Colony Optimization) is used for the route optimization. Ant Colony Optimization is a Swarm Intelligence Technique inspired by the behavior of real ants. ACO Algorithm utilizes the forging behavior of ants (nodes) in order to find the shortest route from source to destination. The nods locates the optimal solution by moving through nodes environment space for representing all possible solutions.

Advantages of Ant Colony Optimization

- ACO algorithm can be used in Dynamic Applications.
- Positive feedback
- Distributed Computation

4.3 Sinkhole Attack Detection Process

In this proposed work, two optimization algorithms ACO (Ant Colony Optimization) and PSO (Particle Swarm Optimization) are used. ACO for the energy consumption is concerned with optimal path selection that needs less energy for routing the data from source to destination. In this mechanism, hash table are used to obtain more accurate suspect list.

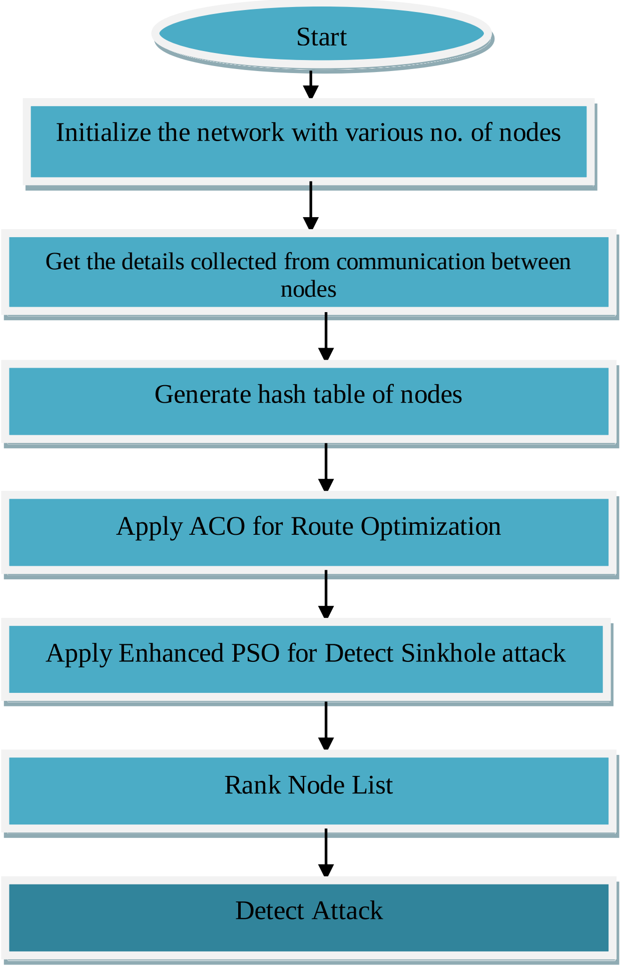

Start
Initialize the network with various no. of nodes
Get the details collected from communication between nodes
Generate hash table of nodes
Apply ACO for Route Optimization
Apply Enhanced PSO for Detect Sinkhole attack
Rank Node List
Detect Attack

Fig 4: Proposed Methodology

Hash table is also used in voting method. PSO method is found to be efficient in sinkhole attack detection. In this the hybrid method of HASH Table and PSO for detect sinkhole attack are used. Hence, the existing PSO is enhanced. MD5 algorithm is used to create hash table. In this method, 256 bit of MD5 algorithm is used. Parameters, namely, throughput, Bit error rate, delay, and energy consumption are used for calculating performance.

V. MATERIALS AND METHODS

This research has developed a novel algorithm for the detection of sinkhole attack using ACO (Ant Colony Optimization), EPSO (Enhanced Particle Swarm Optimization) and MD5 Algorithm.

1.(ACO) Ant Colony Optimization

To find the best route in sinkhole attack detection process one of the effective swarm intelligence technique namely ACO (Ant Colony Optimization) is used.

Ant Colony Optimization is an optimization technique used to find the best path by using the graph. This technique inspired by the behavior of the real ants. It is used to solve computational hard problems. Ants are an individual of the nature with less intelligence looking for the nests to search for food. In this technique, the artificial ants are the agents that search for good solution to a given optimization problems. In ACO ants work in a distributed way with the use of local information; it finds more than one loop free paths between source and destination.

2.EPSO (Enhanced Particle Swarm Optimization)

EPSO (Enhanced Particle Swarm Optimization) is an advanced form of the Particle Swarm Optimization technique. EPSO technique is used to detect sinkhole attack. PSO is a population based stochastic optimization technique inspired by the birds flocking and fish schooling. To primary operators used in PSO are as follows; Velocity vector and position vector. In each repetition, a new velocity value of each particle is evaluated and the value obtained by updated velocity vector is used to calculate the next position of each particle in search space. The formula used to update the velocity “V_t” of position “ X_t” at time “ t ” are as follows:

$V_t+1 = C1V_t+C2.rand1().(X_t-pbest) + C3.rand2().(X_t-gbest)$

Rand1 and rand2 are random values from 0 and 1

In this paper, Enhanced Particle Swarm Optimization is used to detect the sinkhole attack. EPSO performs better than the PSO and ACO. In this technique, hash table are used to conserve more accurate suspect list. Hash buffer is also use in voting method. Hashing has been recently proposed to record the arrangement experienced during recent emphases. All outcomes obtained during a search are collected in a list called the Solution List and the outcomes with the collision are stored in the second list called the Collision List.

3.MD5 (MESSAGE DIGEST 5)

The MD5 algorithm is used to create the hash table. The MD5 algorithm is designed to quite fast on 32-bit machines. The MD5 algorithm does not required any large substitution table; MD5 algorithm is an advanced but slower form of the MD4 algorithm.

MD5 algorithm takes input f any length and produces 128-bit message digest of all the data and the trusted third party registers this digest. The receiver uses this digest to verify the real data.

VI. SIMULATION RESULTS

Simulation has been done in MATLAB R2018A environment and the network performance has been examined with and without optimization and and detection techniques.

Existing performance with the proposed programs in MANET can be determined by examining the quantitative values of the various metrics used to measure the performance of the following protocols:

It is defined as the amount of time taken by data packets to propagate from source to region via MANET. These include possible delays caused by the criticality during route detection, interface queue, and MAC return delays, distribution and transmission times and low delays means better protocol performance.

6.1. Simulation profile

The simulation profile is listed in table below:

Table 2: Simulation Profile

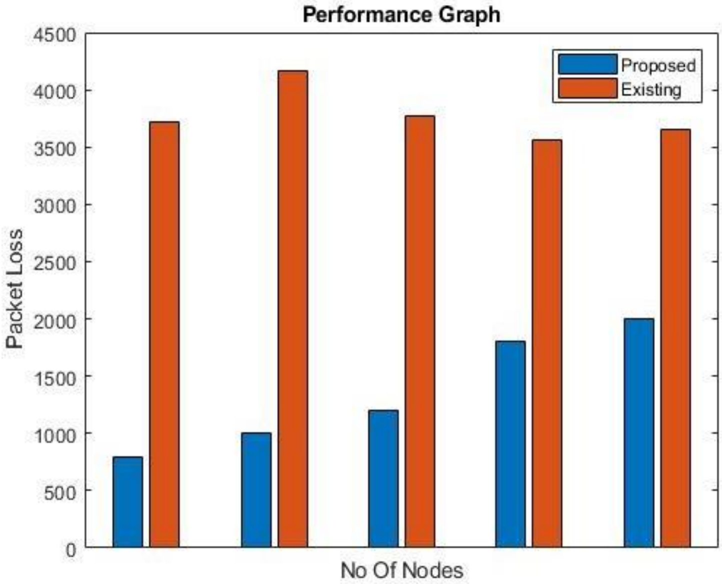
Parameters	Value
No. of nodes	50
Coverage Area	1000*1000
Channel Type	Wireless Channel

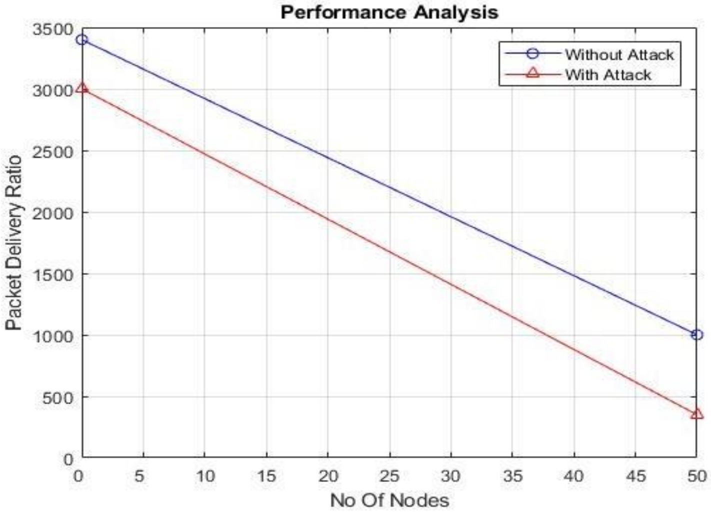
6.2 PACKET DELIVERY RATIO

Estimates of the number of packets received at your destination by the number of packets sent by the source This shows the level of data delivered to your destination. A larger amount of packet delivery rate means better protocol performance.

6.3 NETWORK THROUGHPUT

To exceed the number of data packets delivered to the source to each time zone. Pass is calculated as the minimum received per second as you go.





VII. ANALYSIS

It is an estimate of the number of packets discarded by nodes for various reasons. A lower amount of lost package means better protocol performance.

Lost package = No. packet sent – No. packet received.

Evaluated the performance of the proposed hybrid algorithm with sinkhole & without sinkhole attacks by observing changes occurring with a number of different metrics of performance such as PDR, end-to-end delays, packet loss recovery, and measurement results obtained by a diverse number of network locations from 10 to 50.

VIII. CONCLUSION

Intrusion detection is currently very interesting area of research community. Swarm Intelligence is very useful and effected model of optimization. Ant Colony Optimization, Particle Swarm Optimization, Enhanced Particle Swarm Optimization are the methods of Swarm Intelligence technique. The two methods of swarm intelligence namely EPSO (Enhanced Particle Swarm Optimization) and ACO (Ant Colony Optimization) are used to detect sinkhole attack in MANET. The hash table is used to improve the performance of PSO so this method is called Enhanced PSO. This method performs better performance than existing methods in terms of Throughput, Packet Delivery Ratio, Delay and Packet Loss Ratio. It increases the Packet delivery ratio and decreases Packet loss ratio. The result obtains from this simulation is that this method is more accurate for defending network from malicious nodes.

IX. REFERENCES

[1] G. Keerthana and G. Padmavathi, et. al. "'Detecting Sinkhole attack in wireless sensor network using Enhanced Particle Swarm Optimization technique", in: IJSIA-2016.

[2] Vikash Raina, Sulekha Kumari, Partha Pratim Bhattacharya and V.K. Jain, et. al."The Evaluation and detection of Sinkhole attack by implementing Genetic Algorithm in MANET", in:IJCER- November 2017.

[3] Jeewan Jyoti, et. al." Detection and Prevention of Sinkhole Attack in MANET", in:IJCTT-June 2017.

[4] Iqbal Singh and Harpreet Kaur et. al." Detecting Sinkhole attack in MANET using OLSR Routing protocol with Artificial Intelligence ",in: IJARCS-May –June[2018].

[5] Gisung Kim, Younggoo Han, Sehun Kim, et.al. " A cooperative Sinkhole Detection method for mobile adhoc network", in: Science Direct-January-2009.

[6] Shubh Lakshmi Agrwal, Pankaj Sharma, Rakhi Khandelwal, Sandeep Kumar Gupta, et. al. " Analysis of Detection Algorithm of Sinkhole attack & QoS on AODV for MANET",in:NGCT-2016.

[7] Sarika S, Pravin A, Vijayakumar A, et. al." Security Issues in mobile adhoc networks", in: Science Direct-2016.

[8] Richa Kakucha and Deepak Goyal, et. al." A review on Artificial Bee Colony in MANET", in :IJCSMC-July -2014.

[9] G. Vennila, D. Arivazhagan, N. Manickasankari, et. al. "A Survey of Sinkhole attack on DSR in MANET", in:IJCDMC-May-2014.

[10] Neelam J. Patel, et. al." Detection and Prevention techniques of Sinkhole Attack in MANET: A Survey", in :IJLRET-April-2016.

[11] Shrivastava, L., Bhadauria, S.S., Tomar, G.S. et.al. "Performance Evaluation of Routing Protocols in MANET with different traffic loads" in: International Conference on Communication Systems and Network Technologies. IEEE (2011)

[12] Goyal, P., Parmar, V., Rishi, R.: et. al. "MANET: Vulnerabilities,Challenges, Attacks, Application"' in:IJCEM International Journal of Computational Engineering & Management 11 (January 2011)

[13] Teng, L., and Zhang, Y.et. al. "Secure Routing Algorithm against Sinkhole attack for Mobile Wireless Sensor Network," In Computer Modeling and Simulation, 2010.in: ICCMS'10. Second International Conference on (Vol. 4 pp.79-82). IEEE..

[14]. Tumrongwittayapak, C and Varakulsiripunth, R. et. al. "Detecting sinkhole attack and Selective forwarding attack in WSN". Information Communications and Signal Processing, 2009. In: ICICS 2009, 7th International Conference on (pp.1-5). IEEE.

[15] Fessant, F., Papadimitriou, A., Viana, A.,Sengul, C. and Polamar, E. et. al. "A sinkhole resilient protocol for wireless sensor network: Performance and security analysis". In: Computer Communications, 35(2), 234-248.