RESEARCHERID
THOMSON REUTERS

[Murugesan* *et al.*, 6(6): June, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MULTI ATTRIBUTE MINIMUM THROTTLE APPROXIMATION BASED SINKHOLE DETECTION IN MOBILE ADHOC NETWORKS

R Murugesan[*1], Dr M Vijayaraj[2] & Dr. K. Vetrivel

[*1]ME, Associate professor, Department of ECE, Ultra college of Engineering and technology for women, Madurai 625104

[2]ME ,Ph.D., Professor, Department of ECE, Government college of Engineering Trinelveli 627027

[3]MCA, Ph.D, Anna University Regional Campus, Coimbatore.641046

DOI: 10.5281/zenodo.814697

ABSTRACT

The presence of sinkhole attack in mobile adhoc network affects the quality of service of the network and the problem of mitigating sinkhole attack has been handled with different strategies. Still the methods suffers to achieve the mitigation performance and to overcome this issue, an efficient multi attribute minimum throttle approximation algorithm is presented in this paper. The method performs mitigation of sink hole attacks in distributed manner which improves the quality of service of the network. Each node maintains the trace about node energy, node location, displacement speed, and number of transmission involved. Using all these factors of mobile node, the method computes the minimum displacement factor, minimum depletion factor, and maximum transmission factor. Using all these M3 factors computed, an minimum throttle approximation weight is computed. When the node has higher value than the throttle threshold, the node has been identified as malicious and propagated to the network. The method produces efficient results in sink hole mitigation and improves the quality of service of the network.

KEYWORDS: sinkhole, minimum displacement factor, minimum depletion factor, minimum transmission factor.

I. INTRODUCTION

Sinkhole attack in MANET

The mobile adhoc network combines the wireless nodes with mobility and the nodes are subject to change their locations independently. This freedom movement of nodes makes the topology to change in dynamic manner. This introduces cooperative transmission of data packets and all the nodes perform their own routing to deliver the packets to the destination. This phenomenon makes the nodes to discover the route towards the destination and allows them to choose their own way of transmission. This independency helps the malicious nodes to perform sink hole attack. The sink hole attack is an malicious activity of some nodes which spoils the entire communication of the network. As of the nodes involve in cooperative transmission, each node can communicate with the neighbors. For any sink node, there will be a number of intermediate neighbor nodes. The sink node can be reached only through the specific first hop nodes. The malicious node identify such nodes and try to spoil the neighbor node. Because, each node in the manet has certain fixed energy and to perform each communication the node has to spend more energy.

When a node involve in more number of transmissions, it loose its entire energy and becomes dead. The malicious node identifies such nodes and target towards them. Even though there are number of routes present in the network, the malicious node identifies the particular route and transmits large number of packets to drain its energy. When a neighbor of the sink gets large number of packets it loose its energy and becomes dead. The malicious node tries to make all the neighbors to become dead in short time and spoil the entire network communication. How this has been carried out is through the neighbor discovery. Each node in the manet has same energy and transmission range, but the malicious node comes with higher power and transmission range.

Because of the malicious node has higher transmission range, it can read all the nodes data and can involve in neighbor discovery.

The malicious node involve in all the neighbor discovery and route discovery. Also the malicious node become a neighbor in all the nodes. At the route discovery phase, the malicious node will send the reply as it has the direct route to the sink. This makes the source node to choose the route and allows sink hole attack. Such dangerous threat must be identified and removed from the network. To perform sink hole attack detection, the location details can be used. The location based approach use the location feature and based on that the method would verify the location of the sink hole node. Similarly the energy parameter can be used. Still there are issues in identifying the sink hole attack.

The problem of sink hole attack can be performed with the various features like energy, location, speed, number of transmission. This paper discuss about an efficient sink hole mitigatin technique.

II. RELATED WORK

There are number of methods has been discussed for the problem of sink hole attack detection and this section discuss about various methods.

Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in MANET [1], presents a sink hole detection mechanism which uses the routing protocol as the source to exchange information about the network strategy. The paper also analyses performance of the protocol for sink hole detection.

Sinkhole Attack Detection based on Redundancy Mechanism in Wireless Sensor Networks [2], a redundancy mechanism is presented to prevent the sink hole attack. To detect the suspicious nodes, the method sends messages and according to the reply being received the method confirms the presence of malicious node. The detected node is being evacuated from the list to safeguard the network.

Detection and Prevention of Wormhole attack in MANET [3], surveyed some existing techniques for detection of wormhole and a method for detecting and preventing wormhole attack in MANET is proposed. The proposed approach is based on Smart Packet, wormhole infected nodes can be detected based on acceptance of the smart packets by the nodes in the network. All the simulation will be done on ns2 using AODV routing protocol.

Detection of sinkhole attack in wireless sensor networks [5] proposes a Sybil attack detection scheme which initially uses the consistency of data to find the group of suspected nodes. Then, the intruder is recognized efficiently in the group by checking the network flow information. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified.

Intrusion detection of sinkhole attacks in large-scale wireless sensor networks [6], proposes a novel algorithm for detecting sinkhole attacks for large-scale wireless sensor networks. We formulate the detection problem as a change-point detection problem. Specifically, we monitor the CPU usage of each sensor node and analyze the consistency of the CPU usage. Thus, the proposed algorithm is able to differentiate between the malicious and the legitimate nodes. A sinkhole attack detection scheme in Mintroute wireless Sensor Networks [7], where the vulnerabilities of Mintroute protocol to sinkhole attacks are discussed and the existing manual rules used for detection are investigated using different architecture.

An Approach to Improve the Performance of WSN during Wormhole Attack using Promiscuous Mode [4], proposes promiscuous mode method to detect and isolate the malicious node during wormhole attack by using Ad-hoc on demand distance vector routing protocol (AODV) with omnidirectional antenna. This paper proposes that the nodes which are not participating in multi-path routing generates an alarm message during delay and then detects and isolate the malicious node from network.

Detection and defense of Sinkhole attack in Wireless Sensor Network [8], realizes a mechanism to launch sinkhole attack at wireless sensor networks. And then present some mechanisms to detect and defense this type of attack. Finally, we do some experiments to verify our methods.

Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques [9], address a particular attack to the location and neighbor discovery protocols, carried out by two colluding nodes that set a wormhole to try to deceive an isolated remote WSN node into believing that it is a neighbor of a set of local nodes. To counteract such threat, we present a framework generically called detection of wormhole attacks using range-free methods (DWARF) under which we derive two specific wormhole detection schemes: the first approach, DWARFLoc, performs jointly the detection and localization procedures employing range-free techniques, while the other, DWARFTest, uses a range-free method to check the validity of the estimated position of a node once the location discovery protocol is finished.

A non cryptographic method of sink hole attack detection in wireless sensor networks [10], proposed a scheme to defend against sink hole attacks using mobile agents. Mobile agent is a program segment which is self controlling. They navigate from node to node not only transmitting data but also doing computation. They are an effective paradigm for distributed applications, and especially attractive in a dynamic network environment. A routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sink hole attack. The significant feature of the proposed mechanism is that it does not need any encryption or decryption mechanism to detect the sinkhole attack.

All the methods has the problem of poor classification and less sink hole detection accuracy.

M^3: Multi Attribute Minimum Throttle Approximation based Sinkhole Detection:

The method reads the network trace being maintained and identifies the list of nodes. From the trace available the method compute the number of transmission being involved, minimum displacement factor, minimum depletion factor, and maximum transmission factor. Using all these M^3 factors computed, an minimum throttle approximation weight is computed. Based on computed factors, the method decides the trustworthy of the node. The entire phase has been split into number of stages namely Feature Extraction, DDT Computation, Minimum Throttle Approximation and Sink hole Detection. Each stage will be explained in detail in this section.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

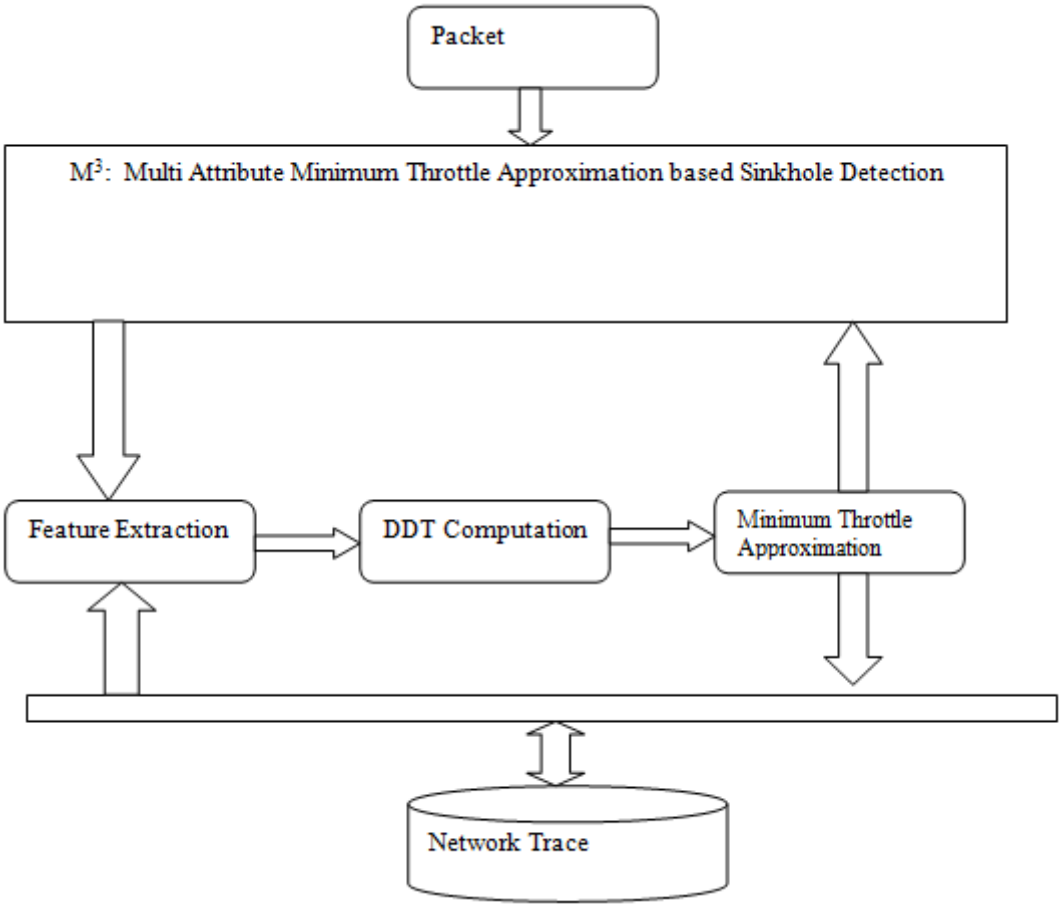


Figure 1:Architecture of Minimum Throttle Approximation Based Sink hole Detection

The Figure 1, shows the architecture of minimum throttle approximation based sink hole detection algorithm for the mobile adhoc networks. Also it shows the functional components of the proposed approach.

III. NEIGHBOR DISCOVERY

At this stage, the method first generates a neighbor discovery request. Generated request has been broadcast into the network. Upon receiving the request which are located within the transmission range of the node, they generates the reply. The reply contains the energy parameter, location and displacement speed. The source node receives the reply till the timer ends and extracts the features from the reply packet. This will be used to perform the approximation at the sink hole detection.

Algorithm:
Input: Neighbor Matrix N
Output: Neighbor Matrix N.
Start
Read Neighbor matrix N.
Generate neighbor discovery request NDR.
Broadcast request NDR.

Initialize neighbor lookup timer NLT.

While (NLT==Running)
Receive NDR-Reply.
Extract NodeID.
Extract Speed.
Extract Location.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Extract Energy.
Add to neighbor table N.
End
Stop.

The above discussed algorithm generates the neighbor discovery message and collects the neighbor details.

Feature Extraction:
The feature extraction is the process of obtaining various features from the statistics. The sink node maintains various logs produced at the reception of data packets. From the logs available, the node extracts the logs belongs to each neighbor identified in the neighbor discovery. For each node, the method splits the logs which will be used to perform DDF Computation.

Algorithm:
Input: Neighbor Table Nt.
Output: Trace set Ts.

Start
Red Neighbor table Nt.
Initialize trace set Ts.
For each node Ni from Nt
Trace set Ts(i) = $\sum Traces \in (Nt).nodeid == Ni$
End
Stop.

The above discussed algorithm generates trace set belongs to each node which will be used to perform DDF computation.

DDT Computation:
The method reads the trace set produced at the previous stage and for each node being identified in the neighbor discovery, the method computes the minimum displacement factor, minimum depletion factor, and maximum transmission factor. The minimum displacement factor represent the node displacement which should be occurred in time according to minimum speed. The depletion factor represent the minimum amount of energy depletion should be occurred according to the number of transmissions. Similarly the maximum transmission factor represent the possible number of transmission could be performed by the node with the initial energy parameter. All these factors are used to perform approximation for sink hole detection.

Algorithm:
Input: Trace set Ts, Neighbor List Nl.
Output: DDT List Dl.

Start
For each node Ni from Nl
Compute number of transmission involved Nt = $\sum Traces(Ts(Ni))$
Compute minimum displacement factor NDisf = $\frac{\text{Nl(Ni).Location} - (\text{Nl(Ni).speed} \times \text{Nl(ni).Initial Location})}{Node.minimumspeed}$
Compute Minimum depletion factor NDepf = $\frac{\text{Nl(Ni).Initiali Energy} - (\text{Nt} \times \mu)}{\mu}$

Compute Minimum Transmission Factor NTf = $\frac{(\text{Nt} \times \mu)}{\mu}$
End
Stop

The above discussed algorithm computes the transmission, displacement and transmission factor to perform approximation.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Minimum Threshold Approximation:
The minimum threshold represents the trustworthy of the neighbor. Even though the malicious node becomes the neighbor, by approximating the displacement, depletion and transmission factors, the presence of malicious node can be identified. The method computes the minimum throttle approximation weight. Based on computed weight a single neighbor will be selected as the carrier.

Algorithm:
Input: DDT List Dl, Neighbor Trace Nt.
Output: Carrier C.

Start
Read neighbor trace Nt.
Read DDT list Dl.
For each neighbor Ni from DDl
Compute minimum threshold weight Mtw.
MTW = $\frac{Dl(Ni).transmission\ factor - Dl(Ni).Depletion\ factor}{Dl(Ni).Displacement factor}$
If MTW>Th // then malicious
Alert as malicious
End
End
Choose the most weighted node Ni.
Carrier C = Node(Max(MTW)).
Stop.

The above discussed algorithm computes the minimum throttle approximation weight to choose the carrier.

Sink hole Detection:
The sink hole detection is performed based on the network trace available. The method first discover the neighbor of the node and for each neighbor the list of traces are separated. Using the separated log, the method compute the displacement, depletion and transmission factor. Based on computed DDF values the method compute the minimum throttle weight to choose the carrier. The method identifies the sink hole node based on the threshold value in the DDT computation.

IV. RESULTS AND DISCUSSION:

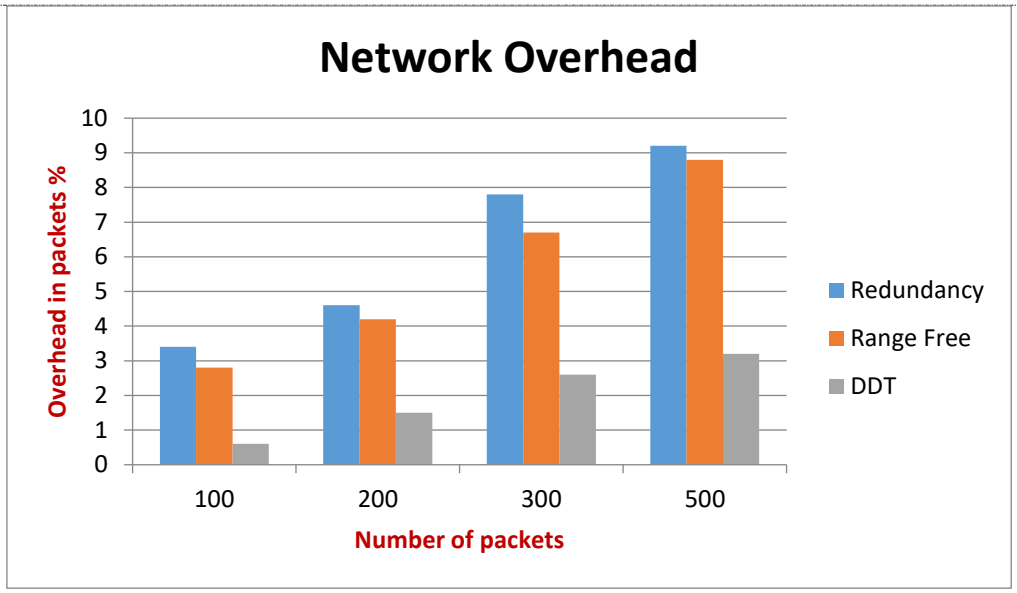
The proposed multi attribute minimum throttle approximation algorithm has been implemented and evaluated with different simulation scenarios. The protocol has produced noticeable growth in the sink hole performance and also reduces the false classification rate. The details of simulation has been displayed in Table 1.

Table 1: Details of simulation

Parameter Name	Value
Simulation Tool Used	Network Simulator Ns2.34
Protocol Name	DDT
Number of Nodes	100
Transmission range	100 meters
Initial Energy	100 Joules
Simulation Time	10 minutes

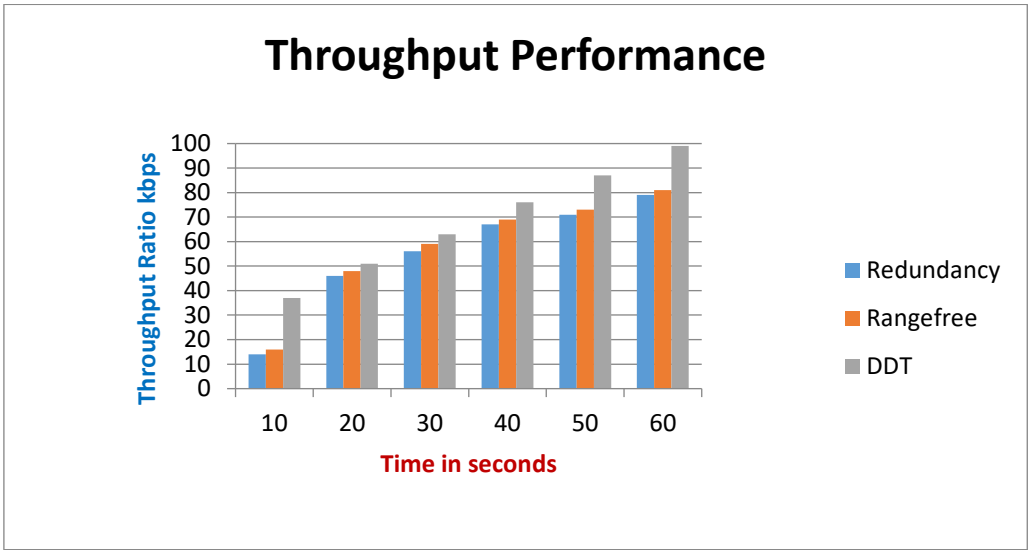
The Table 1, shows the details of simulation being used to perform evaluation of the proposed multi attribute minimum throttle approximation algorithm.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7



Graph1: shows the overhead generated by sinkhole detection.

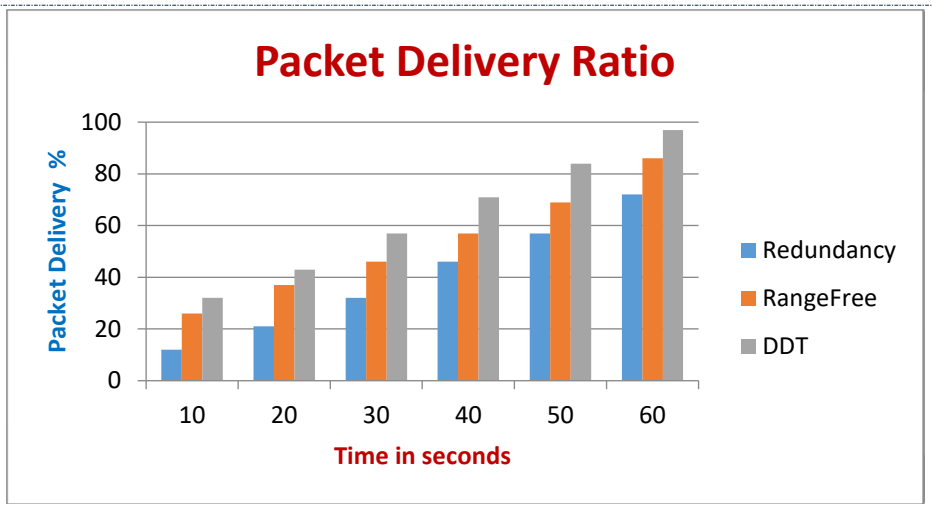
The overhead generated by sinkhole detection process has been shown in graph1. It shows that the proposed approach has produced less overhead than other methods while performing sinkhole detection process.



Graph.2 Throughput ratio of different methods

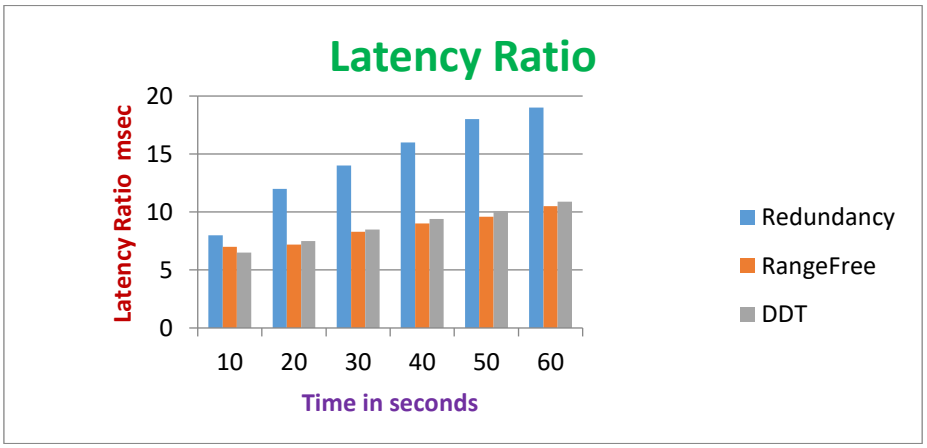
The Graph2 shows the overall throughput ratio of different methods and it is clear that the proposed method has achieved higher throughput than other methods.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7



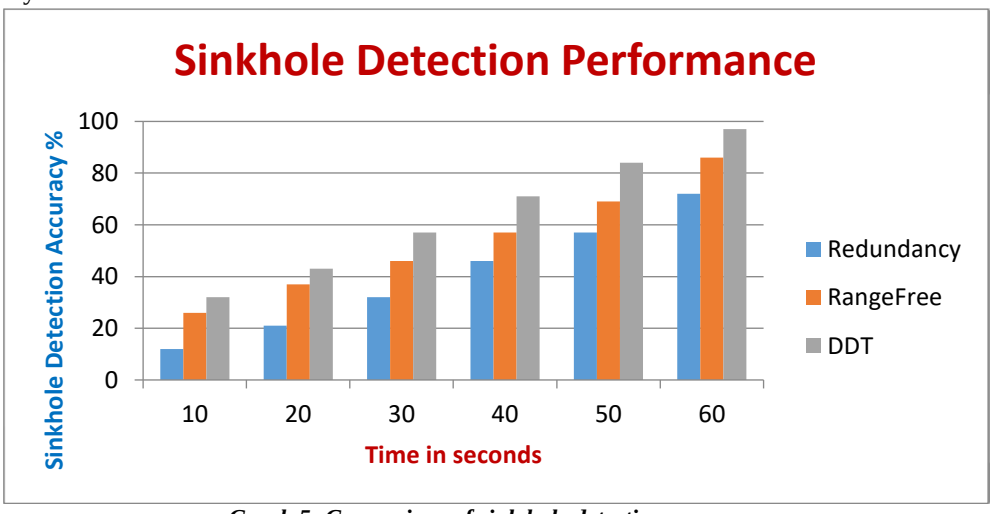
Graph3: Packet Delivery Ratio

The Graph 3: shows the performance of packet delivery ratio of different algorithms and it shows that the proposed method has higher packet delivery ratio than other methods.



Graph4: End-to-end delay

The Graph4 shows the latency ratio of different methods and it shows clearly that the proposed method has lower latency ratio than others.



Graph 5: Comparison of sink hole detection accuracy

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

The Graph 5, shows the comparative result on sink hole detection performance produced by various methods. The result shows that the proposed DDT technique has produced higher detection accuracy than other methods.

V. CONCLUSION

In this paper, an efficient multi attribute minimum throttle approximation algorithm has been discussed. The method identifies the list of neighbors and split the network trace into different sector according to the neighbors identified through neighbor discovery. Then for each neighbor the method compute the minimum displacement, depletion and transmission factors. Using computed factors, t he method compute the minimum throttle weight to decide the malicious node. The method produces efficient results in sink hole detection and improves the network performance.

VI. REFERENCES

[1] Tomar, Chaurasia, Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in MANET, Research gate, manet, 2015.
[2] Fang-Jiao Zhang , Li-Dong Zhai , zhailidong, Sinkhole Attack Detection based on Redundancy Mechanism in Wireless Sensor Networks, Science Direct, Procedia Computer Science Volume 31, 2014, Pages 711-720.
[3] Aakanksha Kadam, Niravkumar Patel, Vaishali Gaikwad, Detection and Prevention of Wormhole attack in MANET, International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016.
[4] M.Choi, H.Choo, Bypassing hole scheme using observer packets for geographic routing in WSNs, in: Proceedings of International Conference on Information Networking, IEEE, 2011, pp.435–440
[5] Salehi. SA, Detection of sinkhole attack in wireless sensor networks, Space Science and Communication (IconSpace), pp: 361-365, 2013
[6] Intrusion detection of sinkhole attacks in large-scale wireless sensor networks, Wireless Communications, Networking and Information Security (WCNIS), pp:711-716, 2010.
[7] Rassam M.A, A sinkhole attack detection scheme in Mintroute wireless Sensor Networks, Telecommunication Technologies (ISTT), pp:71-75, 2012.
[8] Jin Qi, Detection and defence of Sinkhole attack in Wireless Sensor Network [13], Communication Technology ICCT, pp:809-813, 2012.
[9] Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques, International Journal of Distributed Sensor Networks Volume 2012
[10] Sheela D, A non cryptographic method of sinkhole attack detection in wireless sensor networks, Recent Trends in information Technology, pages: 527-532, 2011

CITE AN ARTICLE

Murugesan, R., Vijayaraj, M., Dr, & Vetrivel, K., Dr. (2017). MULTI ATTRIBUTE MINIMUM THROTTLE APPROXIMATION BASED SINKHOLE DETECTION IN MOBILE ADHOC NETWORKS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(6), 455-463. doi:10.5281/zenodo.814697