IJCTA, 9(36), 2016, pp. 315-325

Flow–Based Mitigation for Manet Routing Attacks Detection using Time–Variant Snapshot

M. Vigenesh* and G.Tholkkappia Arasu**

Abstract : Wireless sensor network becomes popular at all levels due to the technology growth with an equal frequency of risk towards various attacks. This paper proposes a novel flow based mitigation model to detect and mitigate routing attacks with the support of time variant snapshots. The sink node monitors the flow and at each time frame it computes the transition traffic pattern which shows the list of sensor node the packet has traveled. From the traffic pattern and with the snap shot of the network which taken at the various time frame, the presence of routing attack and the node which generates the attack could be identified. The sink node maintains the location details of all the nodes in the network, and we assume that the nodes are equipped with similar transmission range and capacities. The geographic and physical features of the nodes has been used to mitigate the manet routing attacks.

Keywords : WSN, Traffic Pattern, Time-Variant Snapshot, Sinkhole attack.

1. INTRODUCTION

Wireless sensor network a high frequent term pronounced by researchers during last decade due to the restrictions of limited energy and deployment nature induces the researchers to think more about WSN. The loosely coupled nature of WSN increases the feasibility of different attacks to be performed by adversaries. One among the possible attack is sinkhole attack which makes the overall traffic be passing through a particular node.

Similarly, the routing attacks which may be raised by the malicious nodes which make the traffic be follow through a long channel where there exist the shortest route available. Also, the malicious node may intend to pass the traffic through a particular node which generates sink hole in the network in order to produce sinkhole attack. Like this various attacks could be produced by generating routing attacks.

The sinkhole attack is one an adversary advertises its neighbors as the only neighbor which has the shortest path to reach the base station. Upon receiving this information what the neighbors will conclude is the adversary is located at most closure neighbor. Hereafter the neighbor nodes forward the packet through the sink which can perform any kind of attack on the network. The adversary can read packets which are coming from compromised nodes and perform the modification, selective forwarding, and selective dropping attacks. So that there is a higher requirement of protocols to detect mitigation of Sybil attacks.

In wireless sensor networks, the intermediate nodes participate in forwarding data packets to reach the destination. Once a group of node compromised with the adversary then the packets are pass through the same path to reach the destination. The higher configured adversary has more power to generate Sybil attack and could participate in a large number of transmission and routing processes. So the traffic pattern

* Research scholar, Department of Computer Science & Engineering, Karpagam University, Coimbatore, Coimbatore

** Principal, AVS Engineering College Salem.

and flow information's could be used to detect the Sybil attacks. Flow-based methodologies have been discussed in many papers in the literature but has not been utilized properly to detect and mitigate the Sybil attacks.

The presence of multiple adversaries makes the traffic pattern to be changed at regular interval. The adversary can generate attack up to the time according to the energy constraint and will go to hell after that. So that the traffic pattern will get change at each time frame. This feature could be used to find out the Sybil attack and adversaries.

The network snapshot which is the most important metric which provides network topology information. The topology of the network will get change at each time frame like the entry of new nodes and death of few nodes. The network snapshot taken at each time frame can be used to identify the presence of an adversary. All this forced us to propose a novel flow based mitigation model for Sybil attack detection. We have used all the above-discussed metrics of the wireless sensor network to find out the Sybil attack and save the network from mitigation.

2. RELATED WORKS

Discovery of sinkhole attack in wireless sensor networks [9] suggests a Sybil attack discovery scheme which initially uses the constancy of data to find the group of supposed nodes. Then, the intruder is documented efficiently in the group by examination the network flow information. The proposed procedure's presentation has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of the algorithm would be verified.

Intrusion discovery of sinkhole attacks in large-scale wireless sensor networks [10], proposes a novel procedure for detecting sinkhole bouts for large-scale wireless sensor networks. We express the detection problem as a change-point discovery problem. Specifically, we screen the CPU usage of both sensor node and examine the faithfulness of the CPU usage. Thus, the future algorithm is able to distinguish between the malicious and the legitimate nodes. A sinkhole attack detection scheme in Mint route wireless Sensor Networks [11], where the susceptibilities of Mint route protocol to sinkhole attacks are deliberated and the current manual rules used for detection are investigated using a different architecture.

An Approach to Progress, the Performance of WSN throughout Wormhole Attack using Promiscuous Mode [2], proposes licentious mode method to perceive and isolate the malicious node during wormhole attack by using Ad-hoc on request distance vector routing protocol (AODV) with an omnidirectional feeler. This paper suggests that the nodes which are not contributing in multi-path routing produces an alarm communication during the delay and then senses and isolate the hateful node from the network.

Detection and defense of Sinkhole attack in Wireless Sensor Network [12], realizes a mechanism to launch sinkhole attack at wireless sensor networks. And then present some devices to detect and defense this type of bout. Finally, we do some experiments to verify our approaches.

Secure Neighbor Discovery in Wireless Sensor Systems Using Range-Free Localization Techniques [13], address an exact attack to the position and neighbor discovery protocols, carried out by two colluding nodes that set a wormhole to try to deceive and remote WSN node into believing that it is a national of a set of local nodes. To counter such threat, we contemporary a outline generically called detection of wormhole attacks by means of range-free methods (DWARF) under which we derive two specific wormhole detection systems: the first approach, DWARFLoc, performs jointly the discovery and localization events employing range-free techniques, while the other, DWARFTest, usages a range-free technique to check the validity of the projected position of a protuberance once the place discovery procedure is ended.

A noncryptographic process of sinkhole attack uncovering in wireless sensor networks [14], proposed a scheme to defend counter to sinkhole attacks with mobile agents. The mobile go-between is a program section which is self-regulatory. They navigate from node to node not only conveying data but also doing

the calculation. They are an effective paradigm for dispersed applications, and particularly attractive in a dynamic network setting. A routing algorithm with manifold constraints is planned based on mobile agents. It uses moveable agents to collect gen of all mobile instrument nodes to make every node conscious of the entire network so that a valid node will not listen to the cheating information from the hateful or compromised node which indications to sinkhole attack. The important feature of the proposed instrument is that it does not need any encryption or decryption instrument to detect the sinkhole attack.

2.1. Problem Statement

Most of the routing attack detection mechanism uses various metrics which are computed based on traffic flow, geographic information and so on. Still, there are problems with the earlier approaches as follows:

Network Overhead Some of the approaches uses control messages to collect the neighbor information which increases the overhead of additional packets transmitted and indirectly increases the traffic and latency in the network.

Throughput : The overhead generated by the earlier approaches due to network overhead reduces the packet delivery ratio and network throughput.

Energy Overhead : The transmission of control messages consumes some energy of all the nodes participates in flooding control messages which reduce the residual energy of all the nodes.

Lifetime : The energy overhead generated by flooding control messages and another protocol support packets reduces the lifetime of the node as well as whole network. Also if there is a centralized routing attack detection mechanism, it affects the energy and lifetime of a particular node or else if it is distributed one then it affects many numbers of nodes.

3. FLOW-BASED MITIGATION MODEL

The proposed routing attack detection mechanism has three different phases namely: Traffic Log Generation- which generates the log about a particular traffic, traffic transition pattern –identifies the traffic pattern which has set of node names to represent the transition path, Time-Variant Snapshot – which generates the topology snapshot of the network and finally Routing attack Detection- which detect the sink node using the results of previous stages.

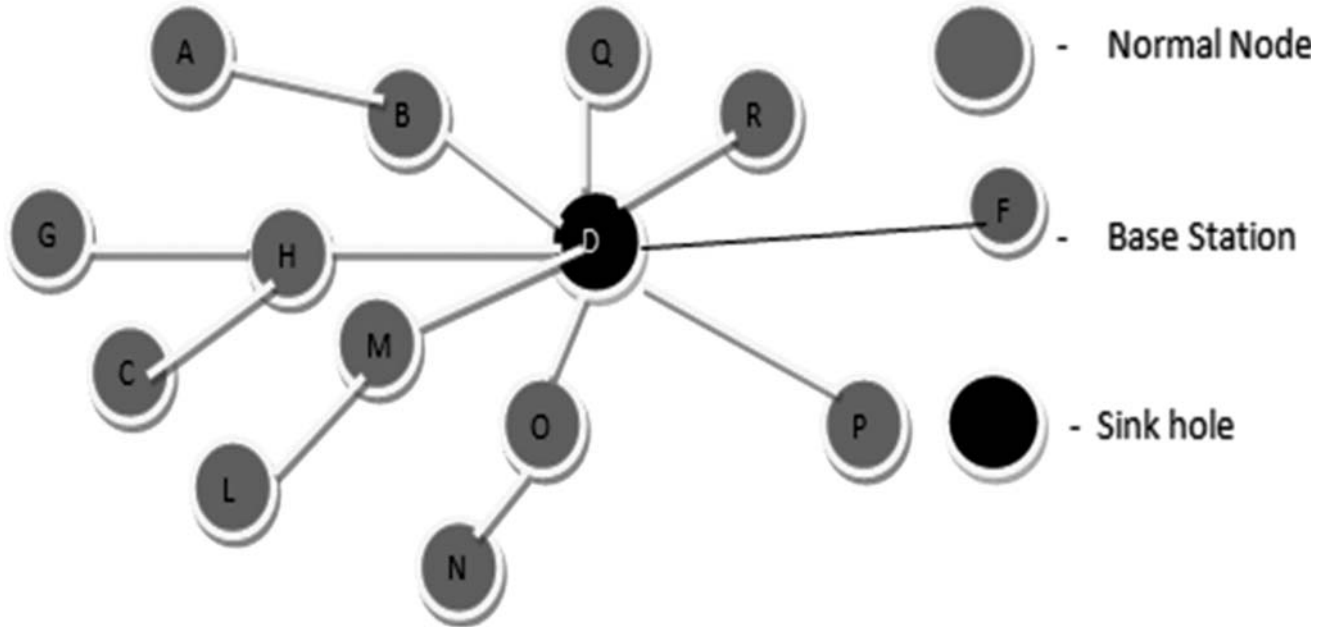

Figure 1: Shows the network topology

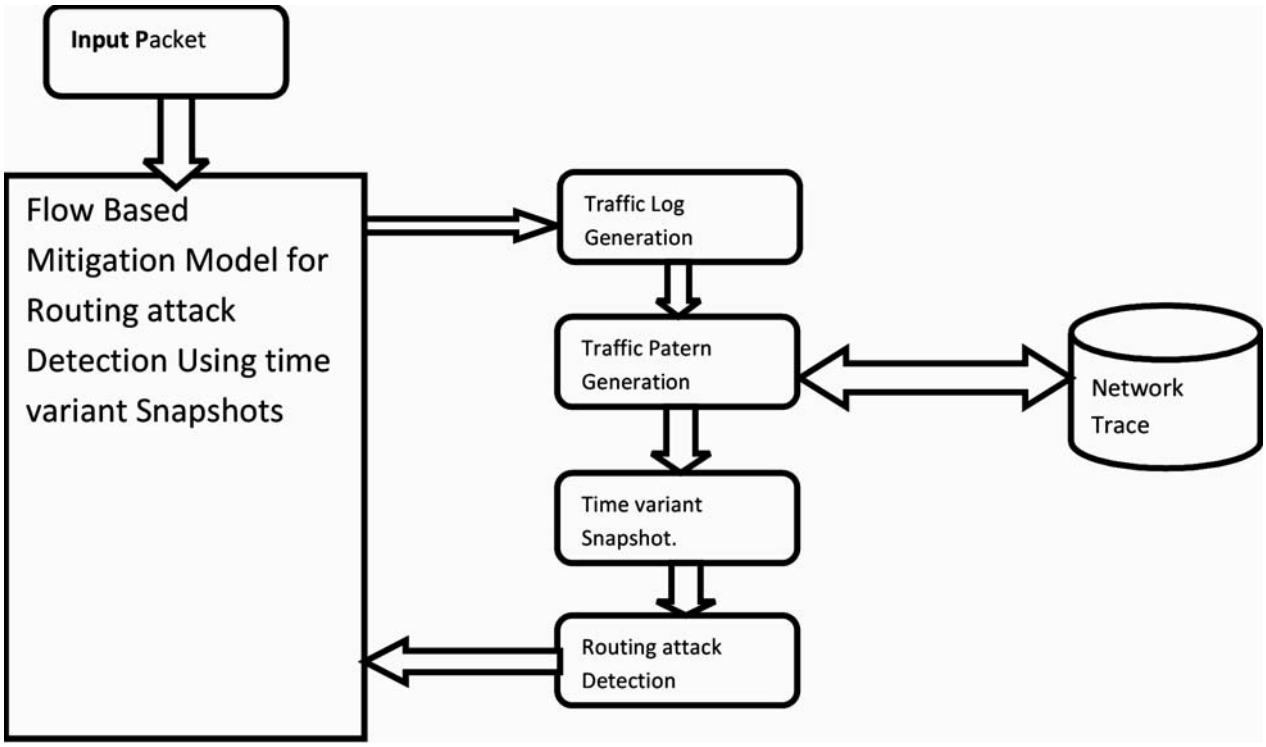

Figure 2: Proposed system architecture

3.1. Traffic Log Generation

We assume that each node forwards the packet towards destination through some of its neighbors and appends the address of its own at the transition field of the packet. The sink node extracts the transition field and computes set of nodes present in the transition path logs to the data base. As shown in figure 2, each node which forwards the packet adds its own address to the transition address field before forwarding the packet to the destination.

Seq.No	TYPE	Data Field	Source Address	Transition Address 1:2:3:4	Destination Address

Figure 3: Shows the packet frame structure used

Traffic Log Generation Algorithm :

Step 1: Start

Step 2: Initialize traffic log TrLog. // TrLog- Traffic Log

Step 3: Receive packet P.

Step 4: If packet Type == Data then

Extract the following fields.

Source Address SA = P(Source Address).

Destination Address DA = P(Dest Address)

Time Received Tr = compute current Time.

Transition address TA = P(Transition Address).

T*r* Log = (∑T*r* Log) + (SA, DA, T*r*, TA)

End

Step 5: Goto step3.

Step 6: Stop.

Table 1

Shows the log generated

Source Address	*Transition Path*	*Destination Address*	*Time*
A	B D	F	13:21:58
G	H D	F	13:21:59
C	H D	F	13:20:18
L	M D	F	13:20:17
N	O D	F	13:20:16

Table1 shows the generated traffic log.

3.2. Traffic Pattern Generation

The transition traffic pattern is computed using the log produced by the base station. The traffic log is cleaned before it used to detect the sinkhole, to overcome the unnecessary memory overhead generated by storing the entire traffic log for prolong period of time. Only a few numbers of traffic pattern will be maintained and at each time frame, a new instance of traffic pattern will be feed into the traffic log table so that the last three-time frame log only maintained at the log table. So that the log file contains the information about packets which are received at few previous time frames. The packets received at a very old time will get deleted.

Table 2

Source Address	***Destination Address***	***Traversal Path***	***Time***
A	F	AB**D**F	13:21:58
G	F	GH**D**F	13:21:59
C	F	CH**D**F	13:20:18
L	F	LM**D**F	13:20:17
N	F	NO**D**F	13:20:16

Algorithm:

Step 1: Start

Step 2: Read traffic log table TrLog.

Step 3: Read traffic transition pattern table Tp.

Step 4: For each log from TrLog

$TrLog_i$ = read log from TrLog.

Extract Source Address SA, Transition path Trp, Destination Address DA, Time T_i from $TrLog_i$

Compute traffic transition path Tp_i = {Source Address, Destination Address Transition Path}.

$Tp_i = \sum Tp + (Tpi + Ti)$

End

Step 5 : for each log from TrLog

If $TrLog_i$ (T_i) < Time Frame end

Delete T_i from Log table.

TrLog = ϕ(TrLog, T_i).

End

Step 6: Stop.

3.3. Time Variant Snapshot

Unlike other geostatic methods the proposed method collects one-time snapshot at the earlier time to get to know the topology information. From the topology information, it generates the snapshot and updates the route table and node table. The route table contains information about a set of nodes and routes to reach other nodes whereas the node table has information about the neighbors of the node. At a later stage, the base station generates the snapshot at regular time interval to detect the presence of sinkhole. Using the traffic pattern which is computed earlier, it finds out a set of nodes which it feels guilty about working condition. From the traffic pattern generated it verifies the presence of each node present in the node table. If it does not find any node, then it sends LifeCycle Message to the guilty node and waits for the reply. Upon receiving the message, the node which has not participate in any of the transmission in particular time window will reply with the message which contains information about the residual energy and neighbors. The control message will be passed to the guilty node only through the longest path which is not present in the traffic pattern. This assures delivery of LifeCycle message at the guilty node and it sends the reply through the path of the request. This procedure reduces the overhead generated by flooding control message throughout the network to collect neighbor informations.

Time variant Snapshot Algorithm:

Start
Init Guilty set Gs, Timer T.
Read Traffic Pattern Table TP, Route table Rt, Node Table N, Snapshot S.
For each node N_i from N
  For each traffic pattern Tp_i from Tp
    Transition path $Trp = \Delta \times (TPi, Tp(\text{Traversl Path}))$
    If Trp ɜ Ni then
    Else
      Add to Gs = $\sum N + Ni$
    End
  End
End.
For each N_i from Gs
  compute Longest Path LP = Max $\left(\frac{RTi}{RT}\right)$
  construct LifeCycle Message Lcm.
  LCM = {Seq.No, Destination Address, Traversal Path – LP}.
  forward packet LCM.
  start Timer T.
  Receive LCMReply from GS_i.
  if LCMReply Received then
    update Neighbor table $\forall (Ni) = N + N_i$.
    update Route Table $\forall (RTi) = Rt + Rt_i$.
    Update Snapshot S.
  Else
  end
end

3.4. Routing Attack Detection

The routing attack detection procedure is executed at regular interval to find out the presence of routing attacks like a sink hole, energy depletion in the network. From the entries of traffic transition table , it computes the common node present in a number of transition pattern. we call this set of the node as guilty nodes Gs, for each from this set we compute the available routes using route table Rt. based on computed routes and the route from traffic pattern Trp, we analyze that whether the route present in the pattern is shorter or not. if the route is longer, then we conclude that there are energy depletion routing attack and sinkhole attack present in the network and another control message will be sent to all the nodes to avoid routing attacks from packet transmission.

Algorithm :

Step 1: Start

Step 2: Read Traffic Pattern Table Tp, read Snapshot S.

Step 3: Initialize guilty set Gs.

Step 4: Compute common node from Tp.

AS-Adversary Set = $N_i(N)$

Step 5: For each Tp *from Tp*

if Tp_i *then*

Ap= computer available path from Route table Rt and snapshot S.

validate the distance of route used and routes from Ap.

if found guilty then

create alert message AM={seq.No,Source Addr, Destination Addr, Sinkhole Addr}

send AM through different path .

end.

end

end

Step 5: Stop.

4. EXPERIMENTAL ANALYSIS

Table 3

The parameters used in our simulation

Parameters	*Value*
Version	NS-alone 2.28
Protocols	**FBRD**
Area	1000m x 1000m
Transmission Range	250 m
Traffic model	UDP,CBR
Packet size	512 bytes

The proposed flow based routing attack detection approach has been implemented in Network simulator NS2. We have designed network topology with different scenarios with a different number of nodes. The proposed methodology has been evaluated with different density networks with multiple maliciouse nodes. The following table 3 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language, and it uses Object Oriented Tool Command

Language (OTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WSN environment consisting of 71 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space operating for 60 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used.

Table 4

Shows the comparison results

S.No	*Number of Nodes*	*Protocol*	*Detection Rate*		*Throughput*	*PDF*
			False +ve	*False -ve*		
1.	71	GEOSTATICAL HAZARD MODEL	3.5	2.5	92	86.70
2.	71	FBRD	0.9	0.8	97.8	93.50

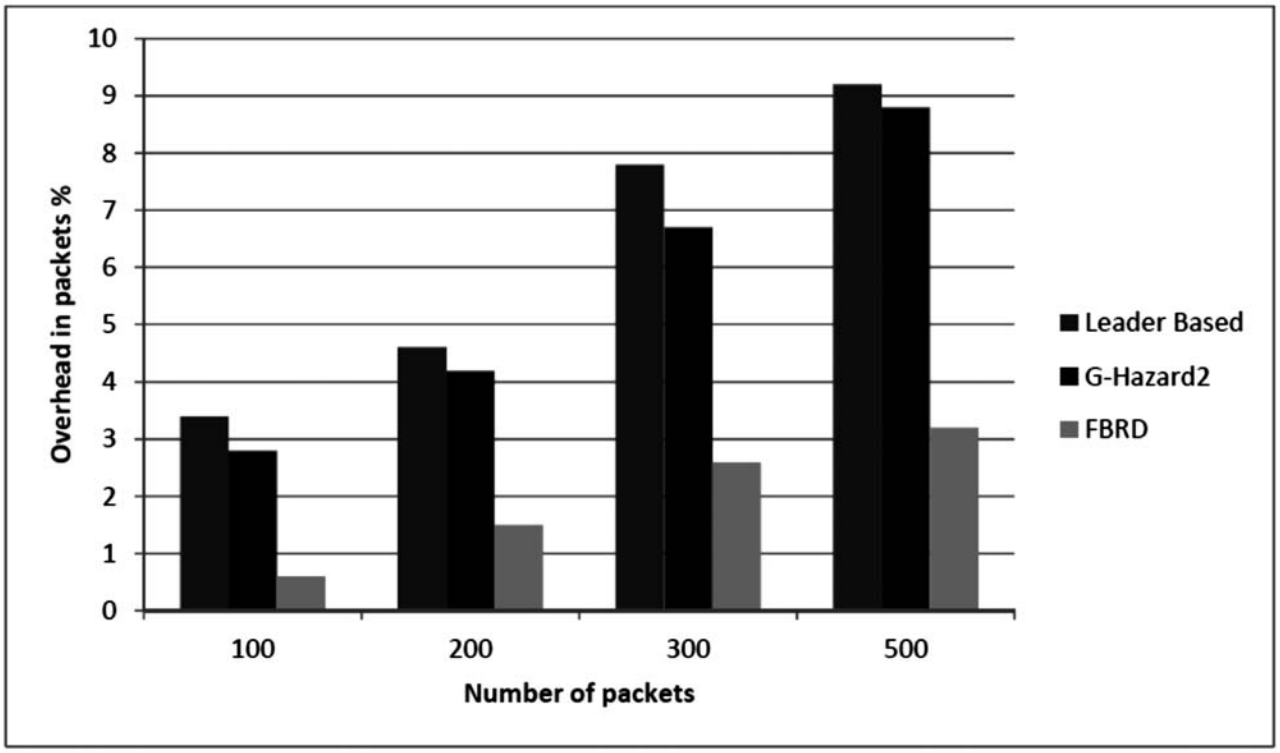

Figure 3: Shows the overhead generated by routing attack detection

The overhead generated by routing attack detection process has been shown in Figure 3. It shows that the proposed approach has produced less overhead than other methods while performing sinkhole detection process.

Throughput performance

Throughput is the rate of packets received at the destination successfully. It is usually measured in data packets per second or bits per second (bps). Average throughput can be calculated by dividing the total number of packets received by the total end to end delay.

The Figure 4 shows the overall throughput ratio of different methods, and it is clear that the proposed Flow based method has achieved higher throughput than other methods.

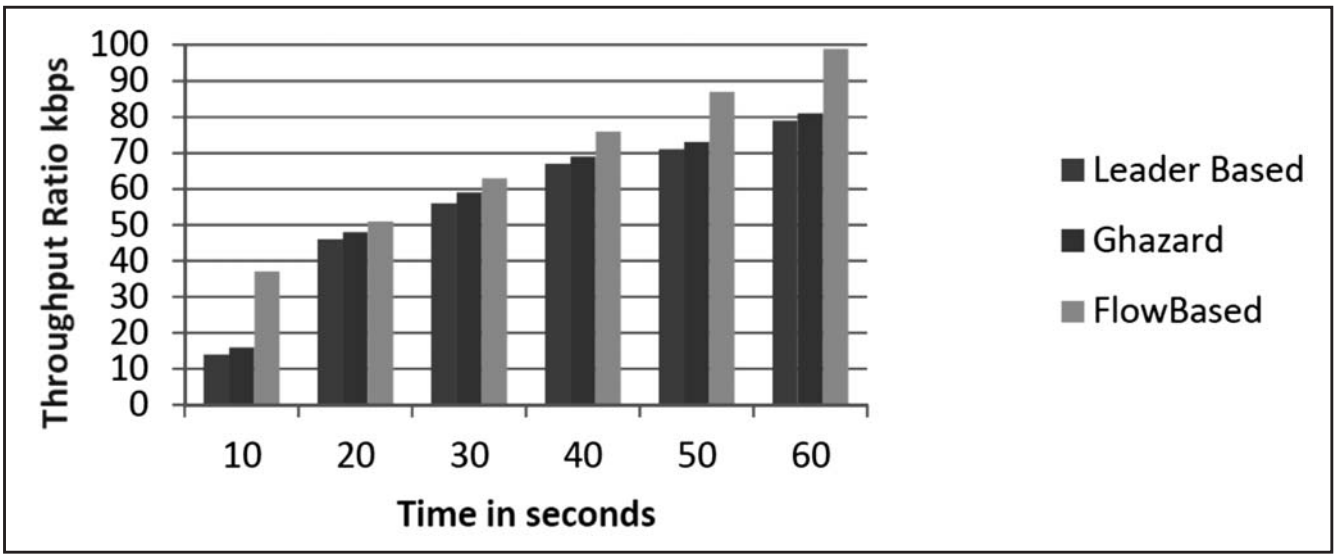

Figure 4: Throughput ratio of different methods

Packet Delivery Fraction

The packet delivery ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node. The packet delivery ratio (PDF) is computed as follows.

PDF = (No. of packets Received/No. of Packets Sent)*100.

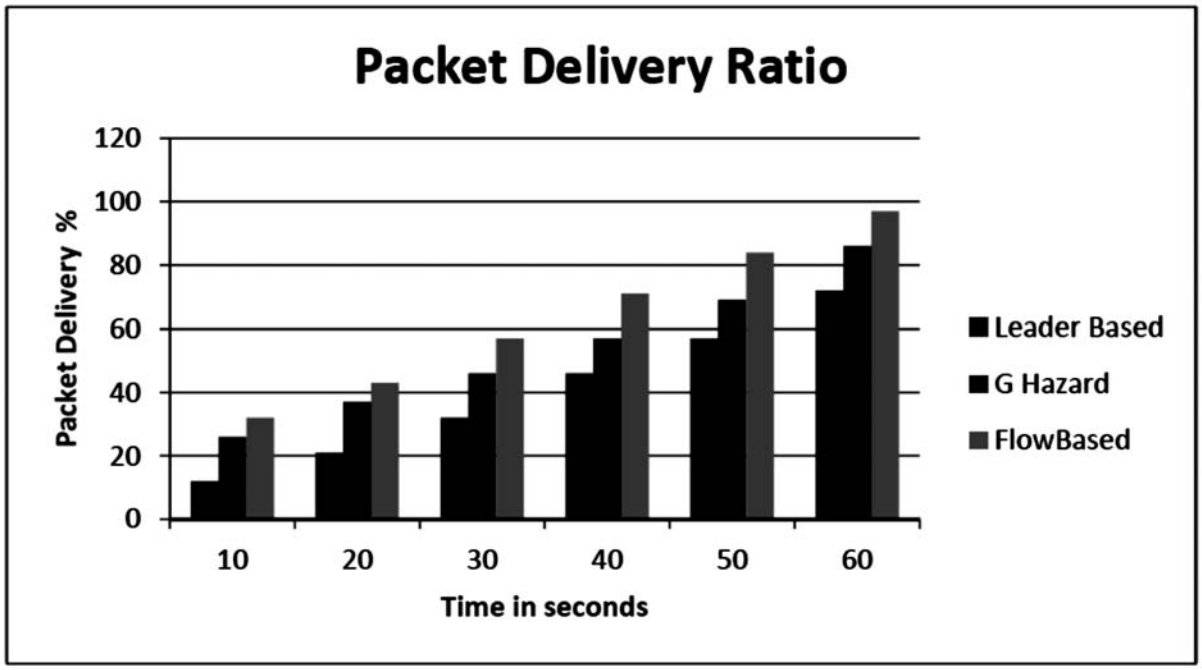

Figure 5: Packet Delivery Ratio

The Figure 5 shows the performance of packet delivery ratio of different algorithms and it shows that the proposed Flow based method has higher packet delivery ratio than other methods.

Average End-to-End delay

Average end to end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, and delay at the MAC due to retransmission, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a MANET from source to destination.

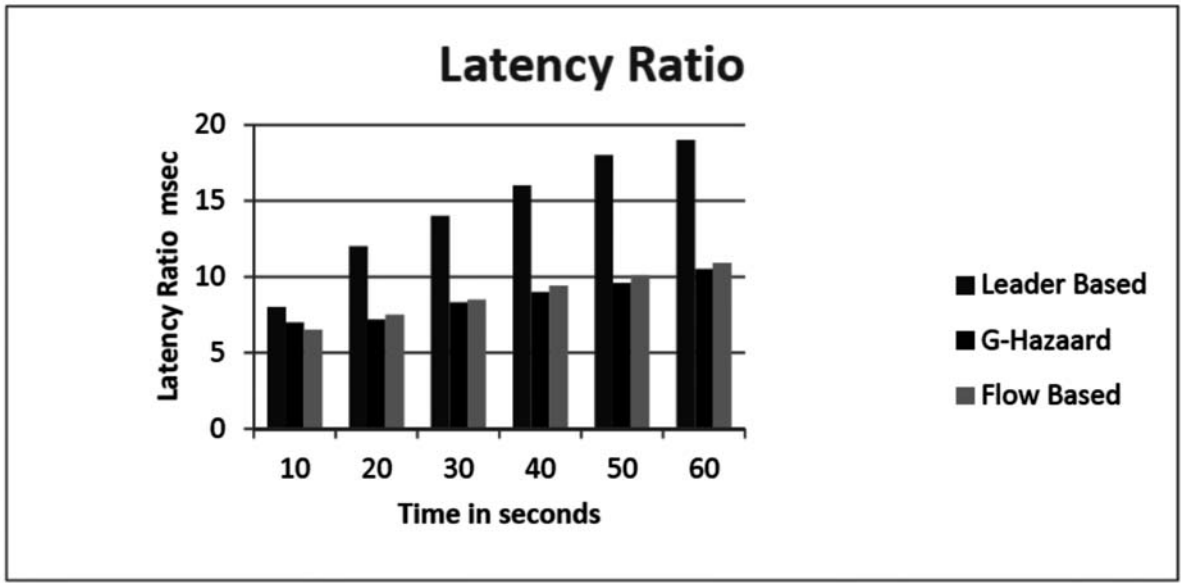

Figure 6: End-to-end delay

$$\text{Delay} = t_R - t_S$$

Where t_R is the receiving time and t_S is the sent time.

The Figure 6 shows the latency ratio of different methods, and it shows clearly that the proposed method has lower latency ratio than others.

5. CONCLUSION

We proposed a flow based mitigation model to detect routing attacks in wireless sensor networks. The proposed method monitors the traffic flow and extract the features of traffic and produces logs into the data set. Then transition traffic pattern is generated to compute the traversal path of the packet. at the third stage, an variant time snapshot of the network is generated using the traffic transition pattern generated . Finally, the mitigation detection is performed using the transition patter and snapshot of the network. We proposed this method with the aim of reducing various control overheads which are generated due to various reasons and particularly by flooding the control messages. The proposed method highly reduces the overhead generated by flooding control messages in the network and increases the performance of the network.

6. REFERENCES

1. F.Yu, S.Park, Y.Tian, M.Jin, S.Kim, Efficient hole detour scheme for geographic routing in wireless sensor networks, in Proceedings of Vehicular Technology Conference, IEEE, 2008, pp.153–157.
2. 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.
3. I.Shin, N.Pham, H.Choo, Virtual convex polygon on based hole boundary detection and time delay based hole detour scheme in WSNs, in: Human Interface and the Management of Information. Designing Information Environments,2009,pp.619–627.
4. C.Baquero P.Almeida, R.Menezes, P.Jesus, Extrema propagation: Fast distributed estimation of sums and network sizes, IEEE Transactions on Parallel and Distributed Systems 23(4)(2012)668–675.
5. R.Villalpando,C.Vargas,D.Munoz, Network coding for detection and defense of sinkholes in wireless reconfigurable networks , in: Proceedings of International Conference on Systems and Networks Communications,2008,pp.286–291.
6. B.Choi,E.Cho,J.Kim,C.Hong,J.Kim,A sinkhole attack detection mechanism for LQI based mesh routing in WSN, in: Proceedings of International Conference on Information Networking, 2009,pp.1–5.

7. I.Krontiris,T.Dimitriou,T.Giannetsos,M.Masuk's,Intrusion detection of sinkhole attacks in wireless sensor networks, in: Algorithmic Aspects of Wireless Sensor Networks,2008,pp.150–161.
8. I.Krontiris,T.Giannetsos,T.Dimitriou, Launching a sinkhole attack in wireless sensor networks; the intruder side, in:Proceedings of IEEE International Conference on Wirelessand Mobile Computing,2008,pp.526–531.
9. Challenges and Authentication in Wireless Sensor Networks by using promising Key Management Protocols" at International Conference in Kristu Jayanthi College, Bangalore on Feb 19th & 20th 2015 and Published in International Journal of Computer Applications
10. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks, Wireless Communications, Networking and Information Security (WCNIS), pp:711-716, 2010.
11. Public Control Algorithm for a Multi Access Scenario comparsing GPRS and UMTS ",at Department of Computer Science and Engineering, National Conference on "Intelligent computing With IoT on April 16 2016.
12. "Teleimersion" Research Journal of Pharmaceutical, Biological and Chemical Sciences on March – April 2016 issue.
13. Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques, International Journal of Distributed Sensor Networks Volume 2012
14. Sheela D, A non-cryptographic method of sinkhole attack detection in wireless sensor networks, Recent Trends in information Technology, pages: 527-532, 2011.