International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Route Inference Based Sinkhole Attack Detection System for Mobile Ad Hoc Networks

T. Poongothai, K. Jayarajan

Abstract: ***Mobile Ad Hoc Network (MANET) is a highly popular wireless network technology due to the proliferation of wireless devices. The characteristic of mobile ad hoc network is described as wireless links and open medium, centralized decision making, dynamic topology, limited power supply, bandwidth constraint and no predefined boundary. Due to its unique characteristics, this technology has been used to support communications in situations where it may be impossible to deploy infrastructure networks, such as military battlefields, disaster recovery sites and medical emergency situations. However, they appear to be susceptible to a variety of attacks than any other networks. The nodes of a MANET communicate with each other with the help of intermediate nodes. Each node of a network act as a host as well as a router. Efficient routing protocols have been developed to support the functionality of each node. These protocols trust that all the nodes are cooperative and well behaved. But some nodes act as a malicious node and launch various attacks on routing protocols. Mainly sinkhole attack affects the routing functionality of the network. Therefore, route inference-based attack detection has been proposed to handle the sinkhole attack in the networks. The proposed system computes the weight value by considering route factor, flow factor and sink factor. Based on the weight value, a malicious node is identified. The experiment results indicate that, the proposed system achieved a packet delivery ratio of 99.6% and throughput of 2700 kbps.***

Keywords: Mobile ad hoc networks, Sinkhole attack, Route Inference, Flow Inference, Attack Detection System.

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is an autonomous system consisting of a group of mobile nodes connected by wireless links without requiring any pre-existing infrastructure. MANET is an attractive technology for many applications with the rapid deployment of the network. The wireless nature and its flexibility lead to a wide variety of attacks. The nodes of a MANET communicate with each other with the help of intermediate nodes. Each node of a network, act as a host as well as a router. Efficient routing protocols have been developed to support the functionality of each node. These protocols trust that all the nodes are cooperative and well behaved. But some nodes act as a malicious node and launch various attacks on routing protocols. Sinkhole attack, Routing attack and Denial of Service (DoS) attack mainly affects the functioning of a Ad Hoc On Demand Distance Vector Routing (AODV) routing protocol. Sinkhole attack spoils all the network connections in mobile ad hoc networks. Further, this attack increases the network overhead and decreases the network lifetime.

An attack is an attempt to bypass the security control of a system or computer network. The attack may modify, release, or deny data (Anjum & Petros 2007). Attacks on MANET severely degrade the performance of the networks. Therefore, there is a need of an efficient mechanism for handling attacks. Providing security to MANET is a challenging task due to the characteristics of shared open medium, dynamic network topology, distributed coordination and resource constrained users. Furthermore, the conventional security mechanisms designed for wireless networks may not be suitable for highly dynamic and resource constrained MANET without modification. Hence, this research introduces a novel attack detection method to secure the MANET.

In the proposed system, route inference theory-based mitigation model is used for network threat detection and mitigation in mobile ad hoc networks. This method works based on the traffic being generated using the traffic log maintained by the sink node. Whenever a packet is being received by the node, it performs route inference, flow inference and sink inference to compute the factor values. Using computed values, weight is computed and based on the value it decides the type of packet. The method improves the performance of mitigation and improves the performance of the threat detection.

The rest of the paper is organized as follows: Section II discusses the related works on sink hole attack detection system. Section III describes the sink hole attack on MANET. Section IV explains the route inference theory-based mitigation model in detail. Section V illustrates the evaluation on the performance and Section VI concludes this paper.

II. RELATED WORKS

In the last few years, mobile ad hoc networks attracted the research community to work on its security services. Many security solutions have been developed to detect the sinkhole attacks in mobile ad hoc networks. Various detection systems have been previously proposed is discussed below.

Usha & Mahalakshmi (2016) have proposed an intelligent technique for detecting sinkhole attack in MANET. This approach applied support vector machines, Fisher Discriminant Analysis (FDA) and artificial immune system for detecting the attack. Apriori algorithm has been used for reducing the number of features.

Revised Manuscript Received on March 30, 2020.
***** Correspondence Author
T. Poongothai*, Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telengana, India. Email: poongothait@gmail.com
K. Jayarajan*, Professor, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women (Autonomous), Secunderabad, Telengana, India. Email: jayarajinfoster@gmail.com

This method used the data collection module, data correlation module, data classification module and analysis module.

Sanchez-Casado et al. (2015) have presented a novel approach to detect sinkhole attack in MANET. This approach is behavior- based detection system that relies on the existence of contamination borders. The performance of the system is analyzed with true positive rate and false positive rate. The main drawback of this approach is collision among malicious nodes. Tunwal et al. (2014) have developed individual trust management technique to detect and prevent sinkhole attack in MANET. In this system, each node is assigned with a trusted weight value. If the node is malicious then the trust value of that node is decremented. Finally, the nodes with lowest trust values are avoided in routing. The performance of the system was evaluated with delivery ratio, throughput and average delay. Identifying malicious node takes more time thus increases the time complexity of a system. Devi & Kannammal (2014) have proposed a distributed and collaborative effort of nodes for sinkhole detection in mobile ad hoc networks. This approach includes the detection of sinkhole existence, detection of sinkhole node and removal of sinkhole node. The drawback of this approach is the overhead involved in extra routing packet flows. Gandhewar & Patel (2012) have proposed a method for the Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network. The performance of this system was observed with packet delivery ratio, end-to-end delay, throughput and packet loss. Usha & Bose (2012) have proposed a novel architecture to analyze the sinkhole attack of mobile ad hoc networks. This method does not provide proper detection mechanism. Kiruthika Devi & Ravichandran (2012) have proposed an intrusion detection system to detect the sinking behavior at MAC layer and network layer using support vector machines in wireless ad hoc networks. To detect sinking attack, the features from MAC layer and network layer has been collected and analyzed. The architecture of this system includes traffic capturing module, data collection module, profile module, detection and prevention module. Joseph et al. (2011) have developed a cross layer based autonomous system for detecting the malicious nodes sinking behavior. These have been used Support Vector Machine (SVM) and Fisher Discriminant Analysis for achieving better accuracy and speed. This method preprocesses the training data for reducing the computational overhead incurred by SVM. A number of features in the training data are also reduced using predefined association functions. The data reduction techniques employed here has made it possible for SVM to be implementable in ad hoc networks. Several experiments are performed considering different network conditions and the behavior of malicious nodes using metrics, such as mobility, traffic density, etc. Jebadurai et al. (2011) have proposed sinkhole detection in mobile ad hoc network using mutual understanding among nodes. This approach considers dynamic source routing protocol. In this method, random assignment of the peak value is not a foolproof technique. Shim et al. (2010) have proposed a cluster analysis method by collecting novel features to detect sinkhole attacks in a distributed manner. DSR protocol of a MANET is considered for feature collection. By considering sinkhole attacks the various features are collected for the detection process. The main drawback of this approach is to collect features only related RREQ message. Kim et al. (2010) addressed the problem of detecting sinkhole attack in mobile ad hoc networks. The malicious behavior of the node is identified with the cooperation of all the nodes. The detection algorithm is composed of three packet broadcasting processes, namely Sinkhole Detection Packet (SDP), Sinkhole Node Packet (SNP), and Sinkhole Alarm Packet (SAP). This scheme uses a sinkhole indicator to detect the routing path of a malicious node. This algorithm broadcasts the packets SAP, SDP, and SNP. The usage of broadcast messages increases the network overhead. Thanachai et al. (2006) have proposed a mechanism for adaptively detecting and defending sinkhole attacks in mobile ad hoc networks by applying trust-based algorithm. This approach uses weights and thresholds for separating suspicious behaviors from normal ones. The disadvantage of this mechanism is the careful selection of the threshold value. Tseng & Culpepper (2005) have proposed two sinkhole intrusion indicators for handling sinkhole attack in mobile ad hoc networks. The first indicator is sequence number discontinuity or duplication. The second indicator is route add ratio. The main drawback of this method is setting an optimal value for sinkhole detection indicators. The attack detection systems discussed in the literature suffers from the presence of malicious node and the node performs eaves dropping and reduces the throughput of the network. The method of dynamic routing has been used in few approaches more susceptible to routing attacks and if there is any malicious node then the whole communication becomes failed. Multi Path routing has been adopted in few methods that suffer from the unavailable route and the overhead of route discovery. Most of the methods suffer from the problem of route discovery and the lack of security. In this method, the throughput is reduced and overhead is increased. Therefore, the work can be extended to improve the throughput and reduce the delay and overhead.

III. SINKHOLE ATTACK IN MANET

Sinkhole attack is one of the most challenging attacks of mobile ad hoc networks. It is a kind of route disruption attack which can spoil all the network connections in mobile ad hoc networks the main aim of sinkhole attack is increasing the network overhead thereby decreasing the network lifetime. A sinkhole attack disrupts the routing in a network by having one device broadcasting that it knows the shortest link to the destination device. In this attack, the malicious node tries to attract its neighboring nodes by broadcasting wrong routing information and receives the whole network traffic as shown in Figure 3.1.

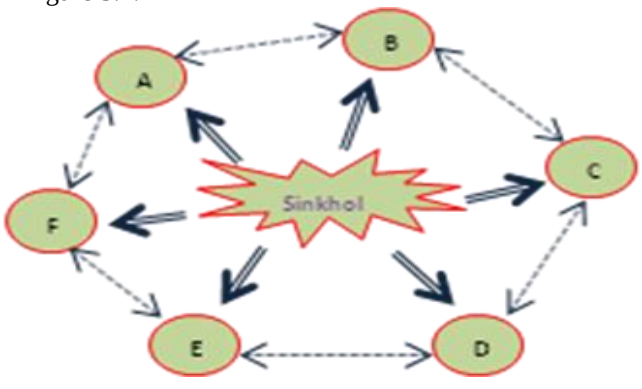

Fig.3.1. Broadcasting wrong routing information

A malicious node uses the sequence number to create wrong routing information. The route introduced by the malicious node seems to be a better path for every hop (Tank & Lathigara 2015). The malicious node trying to deceive a routing path in such a way that legitimate data packets are misrouted. Then it alters the secret information available in the data packet or drops the packets. A malicious node gets the secured data from all the nodes as shown in Figure 3.2.
Sinkhole attack mainly affects the performance of AODV routing protocol by modifying the sequence number and hop count of a routing message.

Fig. 3.2. Receiving data from all nodes

IV. ROUTE INFERENCE THEORY BASED MITIGATION MODEL

Figure 4.1 shows the architecture of Route Inference Theory (RIT) based mitigation model. The theory works on the top of network trace, and the method maintains the network trace of the packet transfer. Also, the trace consists of the details about the route being followed and the packet features. Similarly, the method maintains the log of network information. Using all this information the theory works on three stages namely route inference, flow inference and sink inference. Based on the above information the routing attacks are identified and mitigated.

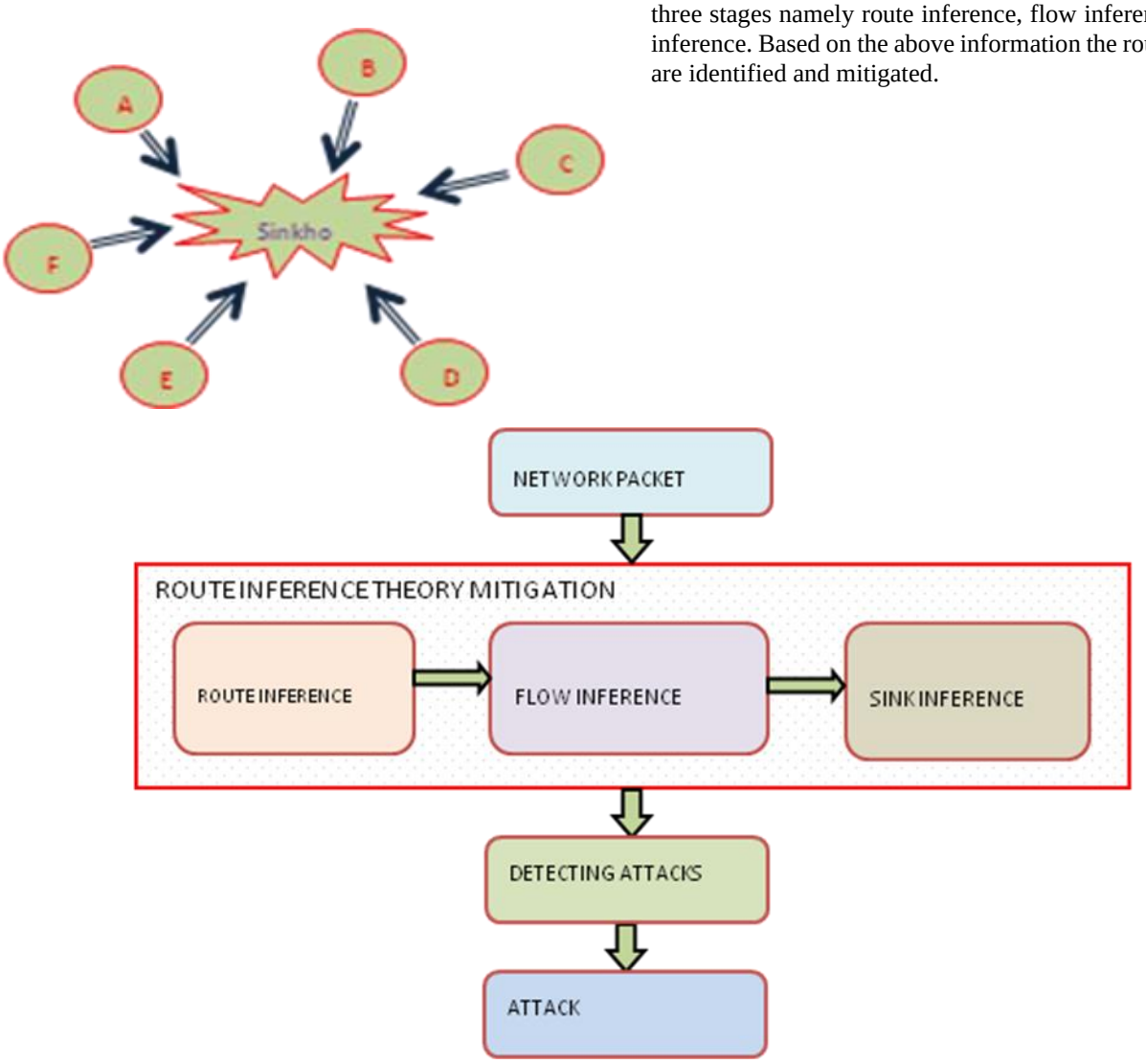

Fig 4.1 Architecture of Route Inference Theory (RIT) based Mitigation model

A. Route Inference

The protocol maintains the trace of packets and the information about the route being followed by the packet. This method reads the trace of routes followed from the source and obtained the list of routes available in the same. For each route, this method computes the route factor which decides the efficient route to transmit the packets. Route factor is computed based on the hop counts, energy parameters of the nodes and traffic in such routes. Based on these values, the route factors for all the routes are calculated and a single route is selected.

Algorithm 4.1: Route Inference

Input: Packet P, Network Trace Nt

Output: Route Factor Rf

Step 1: Start

Step 2: Identify the transmission route from the packet.

$$Tr = \int TransmissionRoute \in P$$

Step 3: Identify all the routes from the source to sink.

Route set Srs = $\int \sum TransmissionRoute \in P$

Step 4: For each route Ri from SRS

Trace Trs = $\int_{i=1}^{sise(Srs)} \sum Trace(Ri) \in NT$

End

Step 5: For each route Ri

Compute average hop count ahp = $\frac{\sum Hops \in SRS}{size(Srs)}$

Compute average energy ae = $\int_{i=1}^{size(Srs)} \frac{\sum energy(Ri)}{ahp}$

Compute average traffic atf = $\int_{i=1}^{size(Srs)} \frac{\sum payload(Ri)}{ahp}$

Compute route factor Rfact =*(ahp × ae) / atf*

End

Step 6: If RFact(Ri) > $\forall$ *(Rfact(SRS))* then

Return 1

Else

return 0.5.

End

Step 7: Stop

B. Flow Inference

The flow of the network has a great impact in the detection of malicious network threats. Each route of mobile ad hoc network has a specific flow and traffic. If a malicious node enters into the network, it tends to transfer the packets in a specific route which spoils the lifetime of the intermediate nodes present in the route. So the detection approach has to identify the flow of the route and could be used to detect the malicious node. The flow inference technique computes the flow of each route by identifying all routes from source to sink. The flow factor value is used for route selection.

Algorithm 4.2: Flow Inference

Input: Network Trace Nt, Route Ri

Output: flow factor

Step 1: Start

Step 2: Identify the transmission route from the packet.

Tr = $\int TransmissionRoute \in P$

Step 3: Identify all the routes from the source to sink.

Route set SRS = $\int \sum TransmissionRoute \in P$

Step 4: For each route Ri from SRS

Compute flow factor Ff= $\int_{i=1}^{size(Srs)} \frac{\sum Tr(Nt).Route==Ri}{size(Srs)}$

End

Step 5: If Ff(Ri)> $\forall$ (FF(SRS)) then

return 1

Else

return 0.5.

End

Step 7: Stop.

C. Sink Inference

The sink node has some neighbor nodes around, and if the source node transmits the packet through particular neighbor then the neighbor would die in early time. This kind of attack would generate sinkhole around the node. By identifying the packets route and number of packets being reached through particular sink nodes, the presence of malicious node can be identified easily. This algorithm identifies the list of routes and packets being reached through them. Using this information, the method computes the sink factor to support network threat mitigation.

Algorithm 4.3: Sink inference

Input: Network Trace Nt, Route Ri

Output: Sink factor Sf.

Step 1: Start

Step 2: Identify the transmission route from the packet.

Tr = $\int TransmissionRoute \in P$

Step 3: Identify all the routes from the source to sink.

Route set Srs = $\int \sum TransmissionRoute \in P$

Step 4: For each route Ri from SRS

Trace Trs = $\int_{i=1}^{sise(Srs)} \sum Trace(Ri) \in NT$

End

Step 5: For each route Ri

Compute sink factor sinf = $\int_{i=1}^{size(Srs)} \frac{\sum Ri.route==Ri}{ahp} \times Nor$

End

Nor = Number of routes available.

Step 6: If Sinf(Ri)> $\forall$ *Ri(Srs)* then

Return 1.0

Else

Return 0.5.

End

Step 7: Stop.

D. Route Inference based Attack Mitigation

At this stage, the method uses all the inference schemes to identify the presence of malicious node. The method computes the route factor, flow factor and sink factor using all the schemes. Using these values, the method computes the weight for the route, if it is found guilty then it announces the network that there exists a malicious node in the route which will be avoided by all the nodes in the network.

Algorithm 4.4: Attack Mitigation

Input: Route Ri

Output: Null.

Step 1: Start

Step 2: Compute Route Factor Rf.

Step 3: Compute Flow Factor Ff.

Step 4: Compute Sink factor Sf.

Step 5: Compute weight

w = Rf×Ff×Sf

Step 6: If w<1 then

Announce malicious

Else

Allow packet.

End

Step 7: Stop

V. PERFORMANCE EVALUATION

Andel & Yasinsac (2016) analyzed the network simulation software packages and suggested some measures for setting up a simulation environment. To validate the efficiency of the proposed IDS model, attacks are simulated with varying network conditions under Linux environment using Network Simulator 2 (NS2). The random way mobility model is used. The MANET is tested by varying the number of nodes from 25 to 150 and node speed varied from 5m/s to 20m/s. The simulation time is 1000seconds and pause time is 400 seconds.The performance of the proposed model is evaluated based on various performance metrics namely, packet delivery ratio, throughput, control overhead, collision rate and end-to-end delay. The performance of proposed model is compared with AODV without attack and AODV with an attack. Figure 5.1 and 5.2 indicates that RIT has a great impact on improving the packet delivery ratio while increasing the number of nodes and speed of nodes in the network. In the absence of an attack, AODV gives more than 97% packet delivery ratio for all network density. However, the packet delivery ratio of AODV declines significantly in the range of 21% to 24% under attack. When RIT is employed under attack, it noticeably achieves the packet delivery ratio of 99.6%. In the absence of attack, AODV gives more than 98% packet delivery ratio by varying the speed. However, the packet delivery ratio of AODV reduces by 4% by varying the speed of nodes. In RIT method the packet delivery ratio is reduced only by 2% by varying the speed of nodes.

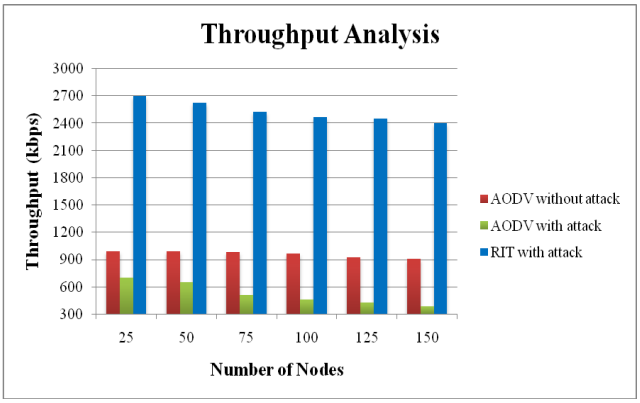

Fig. 5.1 Performance of Packet Delivery Ratio with varying number of nodes

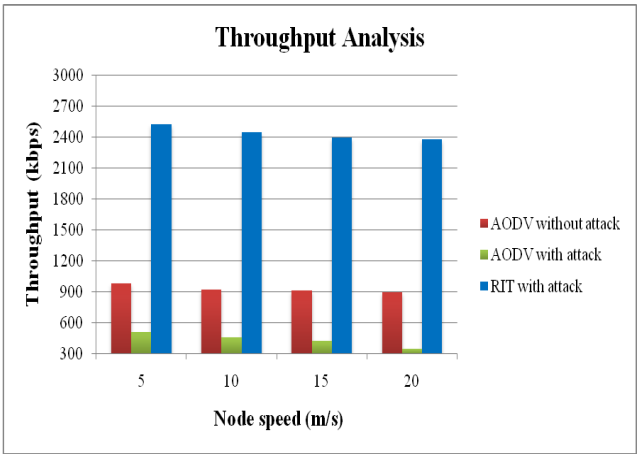

Fig. 5.2 Performance of Packet Delivery Ratio with varying node speed

Figure 5.3 and 5.4 shows the result of throughput by varying the number of nodes and by varying speed of nodes. From the figure, it can be seen that RIT achieves a maximum of 2700kbps in throughput. There is a slight degradation in while varying the number of nodes. The graph shows that speed of nodes affects the performance of throughput under attack. But the performance of RIT is not affected by varying the speed of nodes.

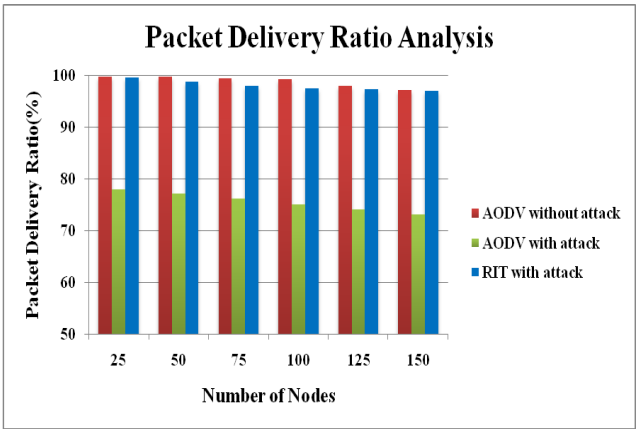

Fig 5.3 Performance of Throughput with varying number of nodes

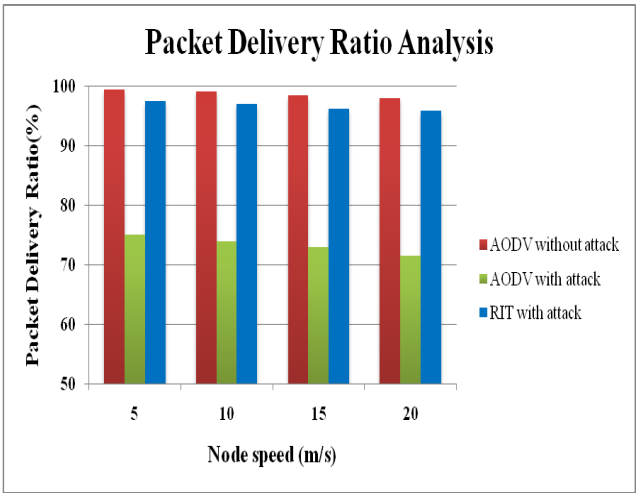

Fig 5.4 Performance of Throughput with varying speed of nodes

Figure 5.5 and 5.6 shows the collision rate of RIT model at a different number of nodes and node speeds. In the absence of attack, the collision rate of AODV is less. If the attack is introduced on AODV the collision rate is very high because all the malicious nodes broadcast forged routing control packets to the legitimate nodes or the malicious nodes trying to receive all data packets. This increases the collision rate of a system under attack. If the detection system is introduced it finds the malicious node and eliminates the unnecessary transfer of routing control packets and data packets.

From the figure, it is clear that the RIT attack detection system reduces the collision rate to 4.25%.

As the number of nodes increases the collision rate also increases because all the nodes trying to send the packets at the same time. From figure 5.3 it is also observed that the speed of node increases the collision rate also increases.

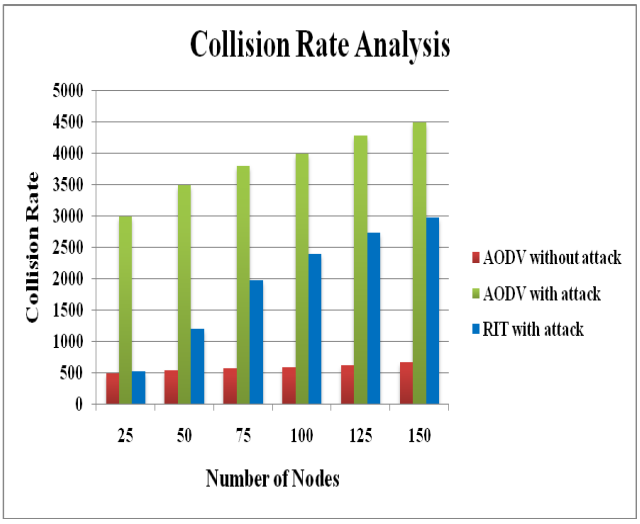

Fig 5.5 Performance of Collision Rate with varying number of nodes

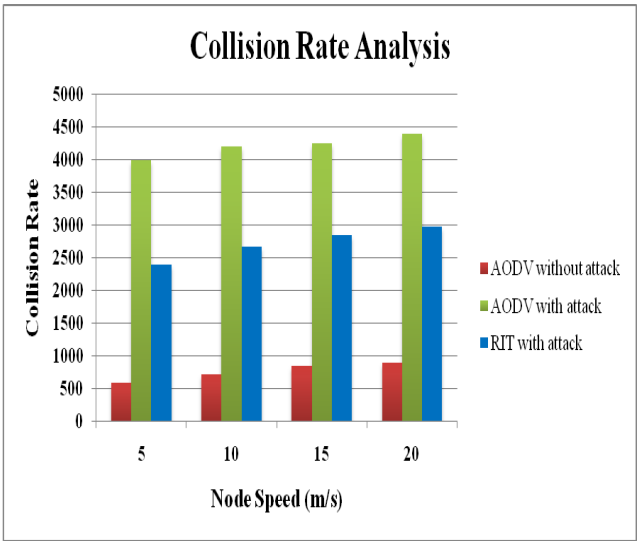

Fig 5.6 Performance of Collision Rate with varying node speed

Figure 5.7 and 5.8 shows the control overhead of proposed system by varying the number of nodes and by varying the speed of nodes. From the figure, it is observed that proposed system has an overhead less than that of a system under attack. As the number of nodes increases, the control overhead also increases as the packet need to be retransmitted whenever there is a loss of packets.

The figure also indicates that the control overhead of RIT model is reduced by 50% compared with AODV under attack with respect to speed of nodes. As the speed of node increases the control overhead is also increased because the packets need to be retransmitted whenever there is an alternate path. But in the case of RIT model, there is a negligible increase in control overhead.

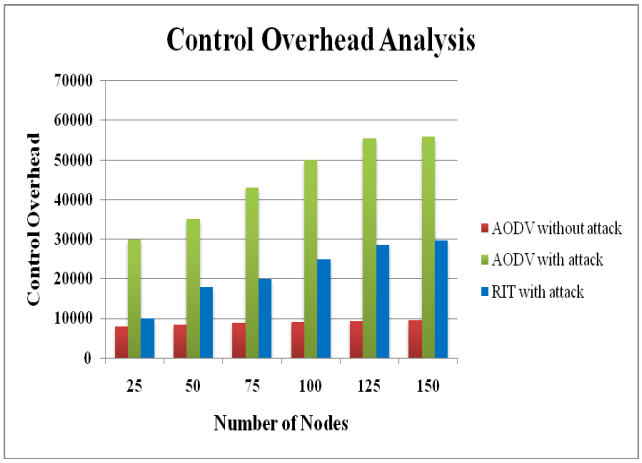

Fig.5.7 Performance of Control Overhead with varying number of nodes

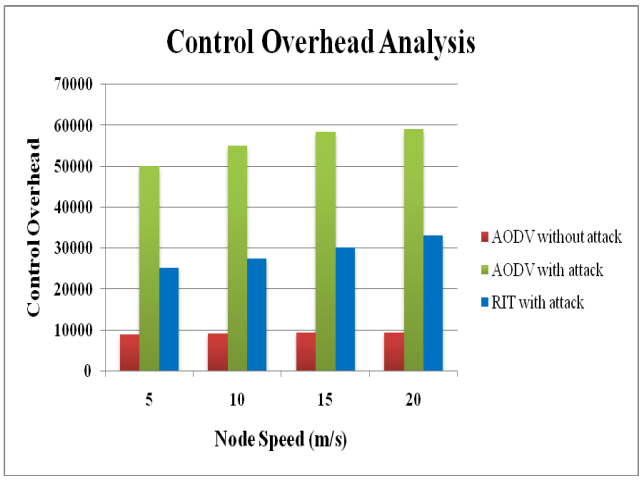

Fig. 5.8 Performance of Control Overhead with varying node speed

Figure 5.9 and 5.10 display the end-to-end delay of RIT model. The figure indicates that end-to-end delay of all schemes increases as the number of nodes increases. When the number of node increases, it requires more time to find the route to transfer the packets. The figure also indicates that the delay of the proposed scheme is superior to AODV under attack. This is because the proposed scheme employs inference mechanism to find the best route to transfer data.

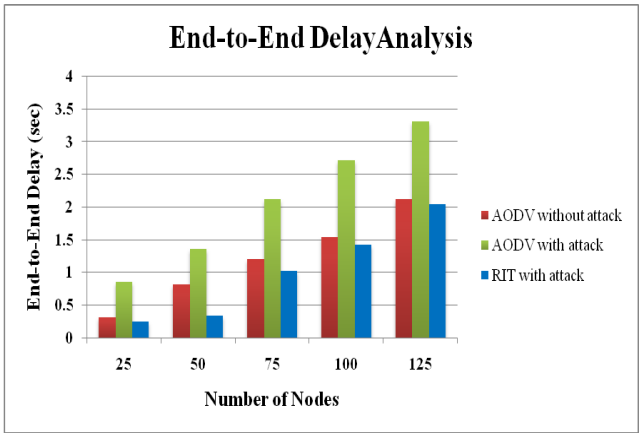

Fig. 5.9 Performance of End-to-End Delay with varying number of nodes

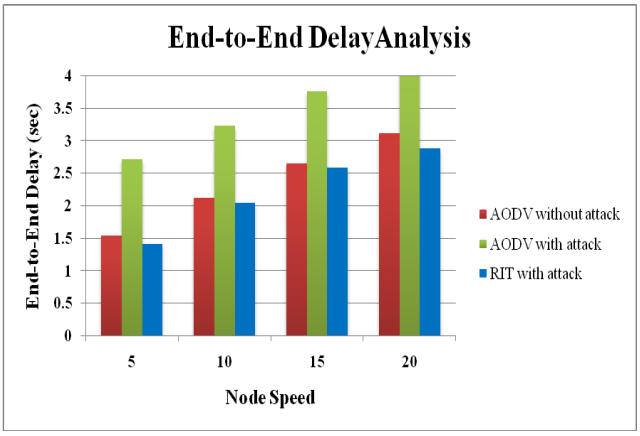

Fig. 5.10 Performance of End-to-End Delay with varying node speed

VI. CONCLUSION

The nodes of mobile ad hoc networks are selfish or malicious in nature due to its limited resources. Detecting abnormal activities of these nodes are not an easy research problem. The dynamic characteristics of mobile ad hoc networks make the detection process as a challenging one. Therefore, a novel attack detection and mitigation method is introduced to protect the MANET. The proposed model introduces a route inference theory-based mitigation model for network threat detection and mitigation in mobile ad hoc networks. The method works based on the traffic being generated using the traffic log maintained by the sink node. Whenever a packet is being received by the node, it performs route inference, flow inference and sink inference to compute the factor values. Based on these inference values a weight factor is computed. If the weight is less than one the route is identified as malicious. This method achieves a packet delivery ratio of 99.6% and throughput of 2700 kbps. Also, this method provides significant performance improvement in reduction of control overhead by 20000 packets, collision rate by 5% and end-to-end delay by 0.6 seconds.

REFERENCES

1. T. R. Andel and A. Yasinsac, "On the credibility of MANETs simulations," Proceeding of IEEE Computer Society Journal of Computers, vo1. 39, no. 7, 2006, pp. 48-54.
2. F. Anjum and M. Petros, *Security for Wireless Ad Hoc Networks*, Hoboken, N.J.: Wiley-Inter science, 2007.
3. N. Gandhewar and R. Patel, "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad hoc Network," Fourth International Conference on. Computational Intelligence and Communication Networks (CICN), Mathura, India, 2012, pp.714-718.
4. J. F. C. Joseph, B. S. Lee, A. Das and B.C Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, 2011, pp. 233-245.
5. J. Jyoti, "Detection and Prevention of Sinkhole attack in Manet," International Journal of Computer Trends and Technology (IJCTT) vol. 48, no. 2, 2017, pp. 45-50.
6. K. Kiruthika Devi and M. Ravichandran, "Detecting Sinking Behavior at MAC and Network Layer using SVM in Wireless Ad hoc Networks," International Journal of Computer Science and Network (IJCSN), vol. 1, no. 3, 2012, pp. 11-17.
7. L. Sanchez-Casado, M. Fernández, P. García-Teodoro and N. Aschenbruck, "Identification of contamination zones for sinkhole detection in MANETs," Journal of Network and Computer Applications, vol. 54, 2015, pp. 62-77.
8. W. Shim, G. Kim and S. Kim, "A distributed sinkhole detection method using cluster analysis," Expert Systems with Applications, vol. 37, 2010, pp. 8486-8491.
9. S. Tahir, S. T. Bakhsh and R. A. Alsemmeari, "An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things," International journal of distributed sensor networks.vol.15, no.11, 2019, pp.1-9.
10. V. Tank and A. Lathigara, "To Detect and Overcome Sinkhole Attack in Mobile Ad hoc Network," Communications on Applied Electronics, vol. 2, no. 6, 2015, pp. 1-5.
11. T. Thanachai, Y. Tapanan and S. Punthep, "Adaptive Sinkhole Detection on Wireless Ad Hoc Networks," *IEEE Aerospace Conference* , Assumption University, Thailand, 2006.
12. C. H. Tseng and B. J. Culpepper, "Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators," Computers and Security, vol. 24, no. 1, 2005, pp. 561-570.
13. K. Tunwal, P. S. Dabi and P. Sharma, "An individual trust management technique for mitigating sinkhole attack in MANET," International journal of computer applications, vol. 95, no.24, 2014, pp. 39-43
14. G. Usha and S. Bose, "Impact of Sinking behavior in Mobile ad hoc network," International Journal of Ad hoc, Sensor and Ubiquitous Computing (IJASUC), vol. 3, no. 3, 2012, pp. 95-104.

AUTHORS PROFILE

Dr. T. Poongothai received her B.E degree in computer Science and engineering from K. S .Rangasamy college of Technology, Tiruchengode, Tamil Nadu in 2001, and M.E Degree in Computer Science and Engineering from College of Engineering, Guindy, Chennai, Tamil Nadu in 2007. She obtained her doctoral degree from Annan University, Chennai, Tamil Nadu. Currently she is working as Professor in the department of Computer Science and Engineering of St. Martin's Engineering College, Secunderabad, Telangana India. She has published around 20 papers in various International journals and conferences. She is member of ISTE and IAENG. Her research interest includes Security issues in Mobile ad hoc Networks, Data Mining, Machine Learning, Deep Learning and Video Analytics.

Dr. K. Jayarajan received his B.E degree in computer Science and engineering from Government College of Engineering, Tirunelveli, Tamil Nadu in 2002, and M.E Degree in Computer Science and Engineering from K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu in 2007. He obtained his doctoral degree from Annan University, Chennai, Tamil Nadu. Currently he is working as Professor in the department of Computer Science and Engineering of Malla Reddy Engineering College for Women (Autonomous), Secunderabad, Telangana India. He has published around 15 papers in various International journals and conferences. He is member of ISTE and IAENG. His research interest includes Security issues in Mobile ad hoc Networks, Cyber Security and Data Mining.