DETECTION OF WORMHOLE ATTACK IN VANET

Mr. Parteek Kumar, Mr. Sahil Verma, Ms. Kavita

Abstract— As security is one of the important issues in Vehicular Adhoc Networks (VANETs), it is required to deal with the threats related to them and one such severe threat is the wormhole attack in which the hacker node grabs the network traffic from one point and directs to another location that may drop the packets. In this paper, a scheme has been proposed which includes the RTT (Round Trip Time), usage level of links and count of neighbors to find the wormhole nodes in VANET. The proposed scheme is assessed and simulated against AODV protocol on NS-2 simulator. The efficiency of the nominated scheme is validated through simulation results.

Keywords— *VANET, Wormhole Attack, Security, Detection*

1. INTRODUCTION

VANETs (Vehicular Ad-hoc Network) are known for creating the self-organised network by allowing the vehicles to communicate with each other in the absence of fixed infrastructure [1]. The communication among vehicles can be done by transferring the messages such as lane change, traffic jam, collision etc. The main goal of VANET is to provide the safety on the roads in order to reduce the collision of vehicles. The safety applications such as traffic signal warning, collision avoidance, road status etc. and the advantages of vehicular communication enhance the security on the roads.

In the past few years, wireless technology has gained popularity in the world of data communication. In fact, the interest in this area has grown considerably. The excitement about vehicular networks is that it deals with the open challenges and provides ample range of solutions. But there are some technical challenges that still need to overcome that are: high mobility, quickly changing network topology, data delivery, speed of vehicles etc. In VANETS, even having so many applications and advantages, there are flaws as well. As VANET lacks infrastructure, so it is susceptible to many attacks.

The one of the most threatening attack is wormhole attack that creates tunnel among two malicious nodes in order to disturb the whole network by silently dropping the packets [2]. Security is the crucial aspect for every field but it is a serious issue in ad-hoc networks. In this attack, two or more nodes cooperate with each other to form a link which is a shortcut and having lower latency, basically they form a tunnel and tries to influence the nodes which are close to these tunneled nodes that these two far distant points are very close to each other. The paper is organized as follow: Section II discusses related work. Section

III provides an overview of proposed algorithm followed by simulation results in Section IV and conclusion in Section V.

2. RELATED WORK

In this section, the details about various research works that has been done to secure VANETs have been discussed. Harikishan et al. [3] proposed a novel approach called IDS (Intrusion Detection System) using Fuzzy inference system to encounter the intrusion behavior within the network. Using Sugeno Fuzzy Inference approach and ANFIS editor, an accurate attack was detected. In proposed work, MATLAB and ANFIS editor is used for experimentation and KDD CUP dataset is used for detecting the anomaly based intrusion with the use of fuzzy inference approach.

V. K. Upadhay et al. [4] proposed a WPAODV technique for the detection and prevention of wormhole. The WPAODV is based on the hybrid model that encapsulates the location, neighbour node and hop count approach. In the proposed scheme, WPAODV extends the AODV by adding one extra feature in it i.e. after detection, WPAODV will bypass the path that is having a wormhole. To detect whether the route is having a wormhole or not, the WPAODV used divide and conquer mechanism over the route recommended by AODV.

R. Karthiga et al. [5] proposed a state traversal mechanism incorporate with finite state machine (FSM) to identify network intrusion with the use of optimized pattern matching algorithm and are also responsible for reduction of memory space required during the implementation of FSM. To achieve this goal, longest common substring algorithm is used and then the outcomes are correlated with the AC algorithm and the bit split algorithm. A. Aggarwal et al. [6] proposed a beacon node mechanism with neighbour node discovery for the detection and prevention of wormhole attack. The proposed technique detects the wormhole by the use of deviation in routing information among neighbours and it does not require any location information and additional hardware.

Chen Ting [7] proposed IDS based on the principle of Back propagation (BP) neural network to solve the efficiency problems such as slow training process and slow detection. S. Eidie et al. [8] introduced an efficient method to detect and prevent wormhole nodes in ad-hoc network using ADOV by utilizing the neighbour information in order to avoid the wormhole. It has followed two phases. In the first phase, all nodes are checked in the route to know that they are 1-hop neighbours or not to find the honesty of the nodes. In the second phase, detection of wormhole is done setting a predefined threshold. If the value

of hop neighbours is found higher than the threshold, then the node is announced as the malicious node.

S. K. Arora et al. [9] presented a combined approach to detect Blackhole and wormhole attack. The combined technique consisted the RTT, buffer length and packet delivery ratio during the routing strategy in order to find the malicious nodes and the malicious routes are prevented by the intrusion detection system (IDS). A. Radhika et al. [10] presented the detection and prevention of DOS attack i.e. Blackhole and wormhole attack in MANETs using Antnet routing algorithm based on ant colony optimization (ACO) scheme. During the wormhole detection, packet leash mechanism has been introduced to detect the wormhole nodes. Although, several detection mechanisms have been proposed by various researchers but still there is no efficient method which can overcome the most of attacks with energy efficient manner and complete accuracy.

3. PROPOSED ALGORITHM

A novel method against wormhole attack in AODV protocol is discussed in detail. AODV protocol is selected for validating the proposed work because it is one of the protocols based on route establishment phase and wormhole attack greatly affects these type protocols.

A. *Short outline of the scheme*

The proposed scheme considers the network to be homogeneous. The variable round trip time between nodes is taken and then the average limit of neighbors is calculated to detect the wormhole link. The proposed method uses no appliances and synchronization of time. While designing the mechanism main focus is to have low energy and bandwidth utilization. The buffer time is also taken into consideration while designing the algorithm. The whole scheme is divided into different stages which are discussed as below in detail.

Stage I: Formulation of neighbor list

1. Every node in the network keeps the information regarding its neighbors (the nodes with which it can communicate directly) with the help of local “HELLO” message. Every sensor node keeps this track by listening to this “HELLO” message at regular intervals of time.

Stage II: Route Establishment and Wormhole Node Suspicion

1. Whenever source node needs to send the message to other node and node is not in neighbor list of source node, latter broadcast a packet which is Route Request (RREQ) and also save the current time of its request message TRREQ.
2. The node when receive the RREQ message and if it is not that node which is target or it do not posses routing entry to final node, it will rebroadcast this message until the destination is not found and also correspondingly save the current time of their RREQ message.
3. When the node having path to destination or destination node itself granted with Route Request Message (RREQ) , that responds with message called Route Reply (RREP). RREP by copying its sequence number field also save its Round Trip Time (RTT) in RREP message (modified). This whole information is then sent to source node.

   The Round Trip Time (RTT) for each node (N_i) is calculated as:

   $RTT\ (N_i) = (T_{RREQ} - T_{RREP}) + PT\ (N_i) + PD$

   Where PT = Processing Time

   PD = Propagation delay due to buffering time

4. Now the source node calculates the RTT between all the nodes which are intermediate to the established path. If the RTT is almost same for each of the link of the established path then there is no wormhole present otherwise there may be wormhole present.
   If the RTT between (N_i) and (N_j) (any two nodes) < Average $_{all}$ then no wormhole present
   Else
   Wormhole may be present
5. Now when the routing table entry is created, the path which is used for highest number of times may indicate about the wormhole link. Although, it is possible the same path is used many a times but presence 6of similar nodes have less probability in routing table entry of many other nodes.

Therefore, by modifying routing table and by adding one more entry of full path for each node can be helpful to be more accurate to find the wormhole link between Ni and Nj.

Go to Wormhole Detection Stage.

Stage III: Wormhole Detection

This Stage has the foundation which is dependent upon the consideration that the malicious wormhole node increments the amount of neighbors in its radius.

Now, if the RTT between N_i and N_j is greater than the average value then there is a requirement of verification.

1. If Number of Neighbors (N_i) and Number of Neighbors (N_j) > Average Neighbor_limit, then the wormhole is located between N_i and N_j, where Average Neighbor_limit is calculated as:

   Average Neighbor_limit = $(N-1)\pi r^2 / A$ [41] ; A = Region Area, N = Node Number, r = radius of transmission.

2. Go to Removal of Wormhole node Stage.

Stage IV: Removal of Wormhole node

1. Send the error message called Wormhole propound to every sensor nodes which are part of network as depicted in Fig. 1.
2.

Type	N	Reserved	Destination count
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Additional Unreachable Destination IP Address			
Additional Unreachable Destination Sequence Number			
Type	Length	Worm_propound	

Fig. 1 Modified RERR message format

2. Whenever this message is received by any node it will remove corresponding id of wormhole node from routing table and the source node restart the process of route discovery with no wormhole node. Flowchart of whole scheme is depicted in Fig. 2.

4. Simulation results and Discussions

In this section, the proposed algorithm is implemented using ns2 simulator [11]. A dynamic set of mobile nodes is considered in order to set up a vehicular environment. The simulation results are discussed. Performance metrics such as throughput, packet delivery ratio and end to end delay are computed. The initial parameters taken during the simulation are represented in the Table I:

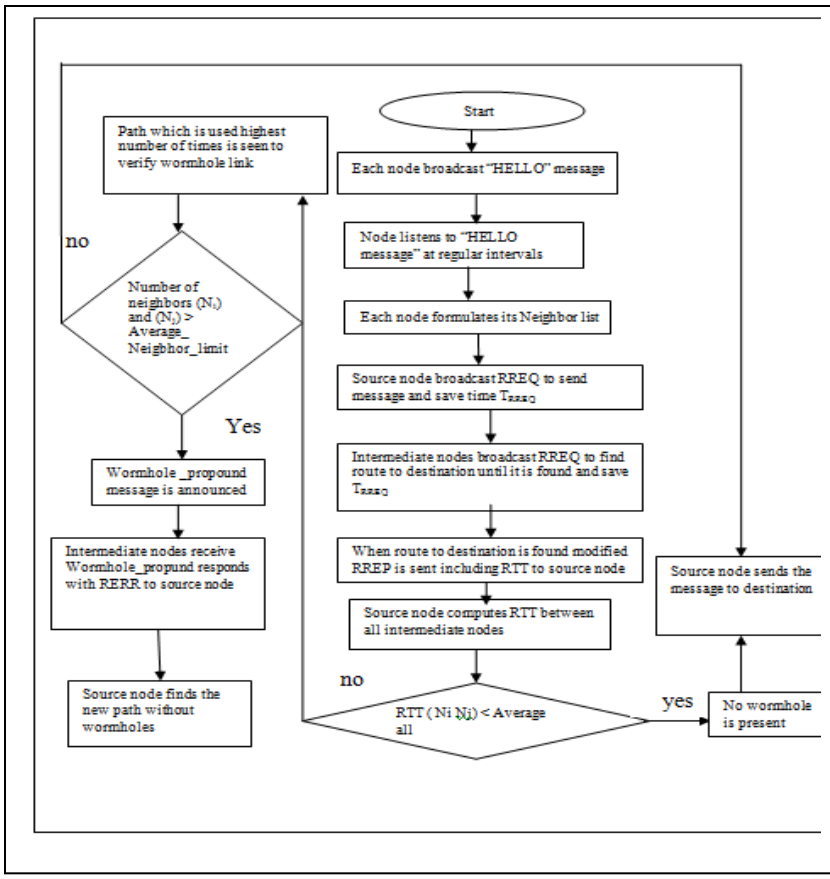

Fig. 2 Flow Chart of proposed scheme

The following Performance Metrics are used for evaluation:

- Packet Delivery Ratio (PDR): It is defined as ratio of the total number of packets received by the destination to the total number of packets sent by the source.
- Throughput: When the number of packets is transmitted from one node to another node within a specified time interval, then it is known as throughput of the network.
- End to End delay (E2E delay): The data transmitted during the average time period from one end to another end.

Packet Delivery ratio is evaluated for the routing protocol AODV, after the wormhole attack and after the proposed scheme deletes the wormhole node. It is

seen as shown in Fig. 3 that the packet delivery ratio is very less in case of wormhole attack as wormhole nodes drops the packet and is considerably improved when the proposed scheme deletes the wormhole node. It is analyzed that the normally the packet loss is nearly 8.74% (91.26 ratio of packets sent to packets received) with 15 number of nodes which is highly increased by two wormhole nodes to nearly 49.5% (50.43 ratio of packets sent to packets received) by dropping the packets. The proposed scheme reduces this packet loss to nearly 15% (84.97). Results depict that PDR is highly dropped by wormhole attack of AODV which is then improved by proposed detection scheme.

Table I: Simulation Parameters

Parameters	**Values**
Simulation Time	400s
Number of mobile nodes	5, 10, 15, 20
Traffic Type	UDP
Topology	Random
Ad-hoc routing protocol	AODV
Size of Packet	1000 bits
Channel type	Wireless
Network interface type	Physical/ Wireless physical
Radio Propagation Model	Two ray ground
Interface Queue Type	Drop Tail
MAC Protocol	IEEE 802.11
Speed	20

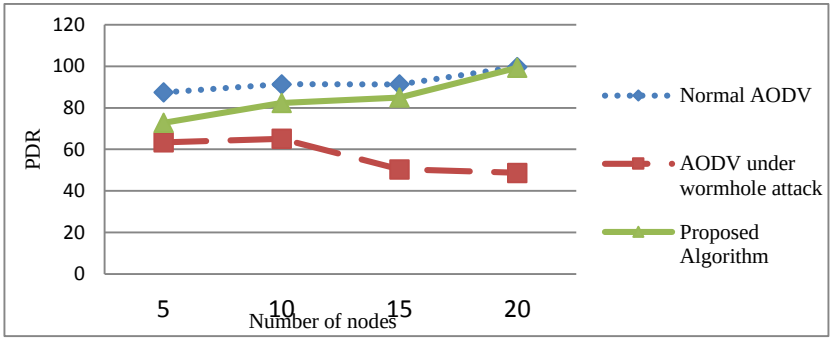

Fig. 3 PDR Vs Number of nodes

Throughput analysis of the network is made for the routing protocol AODV, after the network affected by wormhole attack and after the proposed scheme deletes the wormhole node by varying the node density in the network. It is clearly seen that how the degraded throughput of network is improved by our proposed scheme. The analysis for the same is shown below in Fig. 4. It is analyzed that throughput for the wormhole affected network is reduced to nearly 63 kbps from 88 kbps with 5 number of nodes which depicts that how these wormhole nodes degrades the network performance. The proposed scheme improves the throughput value after detection of wormhole nodes i.e. from 88 kbps to 73.22 kbps. It is depicted from the results that wormhole attack greatly drops the value of normal AODV protocol which is then improved by proposed detection scheme. Average end-to-end delay is also evaluated for the routing protocol AODV, after the wormhole attack and after the proposed scheme deletes the wormhole node in Fig. 5.

Fig. 4 Throughput Vs Number of nodes

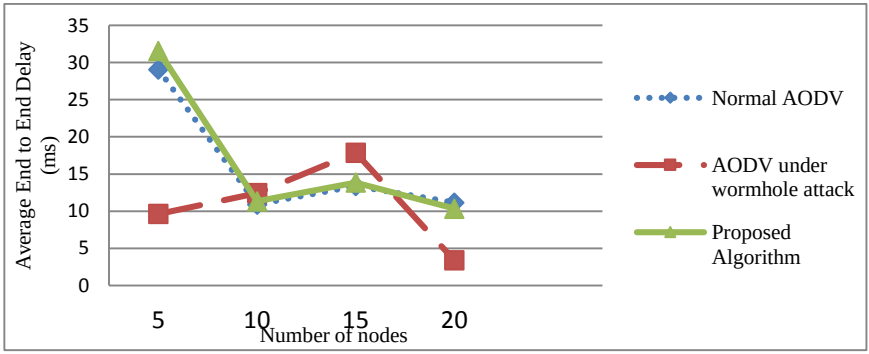

Fig. 5 E2E delay Vs Number of nodes with 2 wormhole nodes

5. CONCLUSIONS

With the emerging technology, VANET is an interesting topic of research having wide variety of applications. Routing faces a lot of challenges in VANETs and because of open wireless nature of these networks there are a lot of security issues. Each node is an independent unit in VANETs, thus each node without sufficient security is prone to be compromised. Wormhole is one such routing attack that disrupts entire network. In this paper, the scheme is proposed which includes the RTT, usage level of links and count of neighbors to detect the wormhole nodes in VANET. The proposed scheme is assessed and simulated against AODV protocol on NS-2 simulator. The efficiency of the proposed scheme is validated through results as the degraded throughput from 17% is raised by proposed scheme to 75%, packet loss rate is reduced to 10 % from 85% after the removal of wormhole nodes.

REFERENCES

[1] A. Singh and M. Singh, "A comprehensive review on vehicular ad hoc network," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 4, no. 4, pp. 462-468, 2015.

[2] R.S. Raw, M. Kumar and N. Singh, "Security challenges, issues and their solutions for VANET," *International journal of Network Security & Its Applications (IJNSA),* vol. 5, no. 5, pp. 95-105, 2013.

[3] A. Harikishan and P. Srinivasulu , "Intrusion detection system using fuzzy inference system," *International Journal of Computer & Organization Trends,* vol. 3, no. 8, pp. 345-352, 2013.

[4] V. K. Upadhya and R. K. Shukla, "WPAODV: Wormhole Detection and Prevention Technique", *International Journal of Advanced Networking and Applications*, vol. 5, no. 3, p. 1922, 2013

[5] R. Karthiga and P. Suresh, "Optimization of Pattern Matching Algorithm for Network Intrusion detection System," *International Journal of Advanced Research in Computer Science & Technology (IJARCST),* vol. 2, no. 1, pp. 20-24, 2014.

[6] A. Aggarwal and A. Saxena, "Wormhole Detection and Prevention Scheme using Beacon Node Mechanism with Neighbor Node Discovery", *International Journal of Computer Science and Information Technologies(IJCSIT)*, vol. 5, no. 5, pp. 6620-6625, 2014.

[7] C. Ting, "Detection system and the realization of the principle of BP neural network based intrusion," in *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, Nanchang, 2015.

[8] S. Eidie, B. Akbari and P. Poshtiban, "WANI: Wormhole Avoidance using Neighbor Information", *Information and Knowledge Technology (IKT), 2015 7th Conference on*, pp. 1-6, 2015.

[9] S. K. Arora and H. Monga, "Combined Approach for the Analysis of Black Hole and Worm Hole Attack in MANET", *Indian Journal of Science and Technology*, vol. 9, no. 20, 2016.

[10] A. Radhika and D. Haritha, "Detection and Prevention of Blackhole Attack, Wormhole Attack in MANET Using ACO", *International Journal of Engineering and Applied Sciences (IJEAS)*, vol. 3, no. 1, 2016.

[11] E. Altman and T. Jimenez, "NS Simulator for beginners," in *Lecture notes*, France, 2003.

AUTHORS' PROFILE

Mr. Parteek Kumar

He has Done B.Tech From Kurukshetra University Kurukshetra. He is doing Teaching in Himalayan Group of Computer sciences Under HPTU Hamirpur and HPU Shimla. He is the faculty member of MCA/BCA Deptt. He has total 1 year 4 months experience.

Mr. Sahil Verma

He is Assistant Professor in E-Max institute of engineering. He has total 5 Years Experience in teaching Area. He Has Publish many Research Papers in National And International journals.

Ms. Kavita

She is an assistant Professor in E-Max institute of engineering. She has total 5 years of Experience in teaching area.