ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

FAKE ACKNOWLEDGEMENT ON CYBER PHYSICALSYSTEM DTN

Mrs.P.Anadavalli[1],
Assitant Professor,
Department of ECE
University College of Engineering,

L.Kayalvizhi[2],M.Priyadharshini[3]
UG Scholars-ECE
Department of ECE
Panruti.University College of Engineering, Panruti.

Abstract: A probabilistic misbehavior detection scheme, for secure DTN routing toward efficient trust establishment. Nodes may misbehave either because they aremalicious. Approach is used in parallel to generate the list of misbehaving nodes. For efficient improvement of scheme, correlate detection pr-obability with a node's reputation.The analysisand simulation results demonstrate the effectiveness and efficiency of the proposed scheme using AODV Protocol.

Keywords : AODV Protocols, MANET, Wormhole attack, Wormhole detection techniques

I.INTRODUCTION

Cyber-Physical systems (CPS) have attracted much interest from both academic and industrial communities in the past few years. A wide spectrum of applications of CPS can be found in areas such as smart grid, intelligent transportation and environment monitoring [1] with the integration of sensing, control, communication and computation. In most CPS infrastructures, wireless sensors are key components with advantages such as low cost, easy installation, self-power [2], when compared with traditional wired sensors. Therefore, wireless sensors have been increasingly equipped in CPS to replace wired ones.

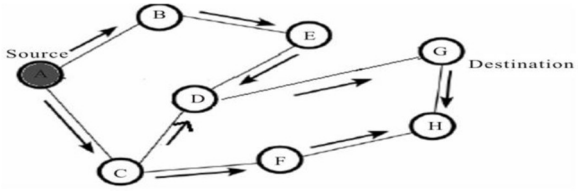
There is a fake acknowlegdement attack in cyber physical systems. The MANET is used to detect the fake acknowlegdement attack.MANETs is a collection of dynamic mobile nodes. It is a structure less network in which mobile nodes are free to move in any direction. There is no any centralized controller in network. A communication have been established which each other using a multi hop links. It behaves like a router. There is no any base station. It is useful in many situations where lack of fixed network infrastructure, such as an emergency situations or rescue operation, medical assistance, disaster malicious node is very hard because mobile node has volatile nature.

Mobile Ad Hoc Network

Delay Tolerant Network (DTN) is used in this scheme because of its store and forward method, which have the qualities of Intermittent connectivity, Long/Variable delay, Asymmetric data rate, High error rate.

AODV ROUTING PROTOCOL

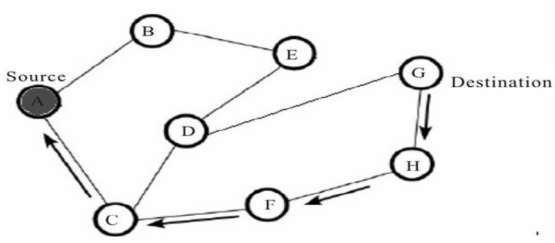
Ad hoc on-demand distance vector (AODV) is a reactive routing protocol which is designed for ad hoc network. Route is not predefine it established when it's needed. AODV routing protocol is used for both unicast routing as well as multicast routing. AODV uses a sequence number for find the routing message is fresh. It applies a destination sequence numbers for finding the fresher pathIt has three types of controlling message RREQ, RREP, RERR.



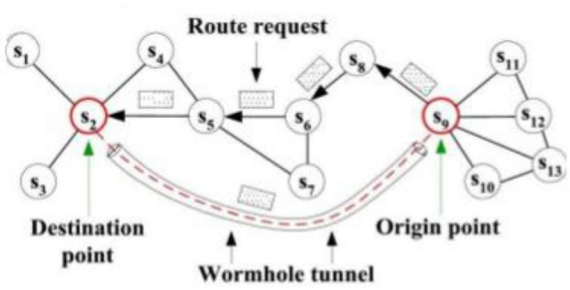
RREQ Broadcast

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018



RREP Forwarded Path



Wormhole attack

WORM HOLE ATTACK

Among various attacks, worm hole is very dangerous as it does not exploit any other node in the network. Due to wormhole attack on proactive type of protocol like AODV first it generates the tunnel between two malicious nodes. In this tunnel it contains data packet for a long time so in result End –to –End delay is affected. In both proactive and reactive routing protocol wormhole attack has significant impact. It performs an operation like packet dropping while it shows in low network throughput.

Tunnel is being generated by using out band or in band channel. Tunnel tried to show direct path between source and destination. This make the tunnelled packet get there either faster or with minimum hops compared to the simple multi hop path on which packet will be transmitted. This creates a false impression crated by this comparison that the two end points of the tunnel also say wormhole points are very close to each other means that that one is a shorter route.

In the following figure s2 and s9 are two malicious end nodes that makes wormhole tunnel to received RREQ packets Malicious node s9 send a packet with a fake route which is s9 to s2, which is not an actual path. Actual path is s9-s8-s6-s5-s4-s2. Route s9 to s2 creates false impression

II.RELATED WORK

The various techniques used for the prevention and detection of wormhole attack in MANET is described below:

Packet Leashes

In this paper [6], the method is used to detect wormhole attack, Temporal Leashes and Geographical Leashes. Temporal Leashes is used a sending and receiving mechanism. Geographical Leashes is based on location of nodes.

1. Temporal Leashes: All modes must need strongly synchronized clock. It is based on off- the -shelf hardware.

2. Geographical Leashes: There is no requirement of clock synchronization. It requires GPS hardware.

Directional Antennas

It is a hardware based approach [7] in which each node are used directional antennas for communication purpose. Use specific sectors of antennas and observe the direction of received signal. This technique fails if an attacker intentionally places the wormhole between the communicating nodes.

Neighbor Node Analysis

In this paper [10] neighbor node approach analyze the entire neighbor node for the purpose of authentication, so that secure transmission can be occur over the wireless network. This method is use request and response mechanism. Node send a request to all neighbor nodes. The node will maintain a table which store a reply time. If reply time is not accurate there is a harmful node in the current

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

network. Comparison is done between the response time of RREP message and the response time of actual message sent. If response time of actual message is greater than the response time of RREP + threshold value than we can say that wormhole link is present in the route. Comparison of this process is repeated continuously till the destination reached.

DelPHI Technique

Delay Per Hop Indication [9] is based on the calculation of (delay per hop) value of disjoint paths. It is based on the fact that, the delay a packet experiences in propagates one hop should be comparable along each hop path. While in the wormhole attack, delay for propagating across fake neighbours are high as there are many hops between them. It doesn't need any extra hardware or tight time synchronization and has high power efficiency [9]. It works for both In-Band and Out of –Band mode.

WHOP Technique

WHOP technique in which a node send extra packet which is called hound packet after the route request is send. From source to destination there are many routes available but the hound packet is processed by the packet in which the packets are involved with source to destination. It contains other three column address of node processing bit (PB) and count to reach next hop (CRNH). It represents the hop difference between neighbors of one hop separated node. At each node CRNH value is increment + 1 from the first.

III.PROPOSED SCHEME

Mobile ad hoc networks (MANET) rely on the cooperation of all the participating nodes. AODV protocol itself incurs a low checking overhead. We calculate the dropping and losing packet size, packet delivery ratio for optimal estimation. Path tracing algorithm to detect the malicious attack using per hop distance and pixel wise measurement. So we can detect accurate misbehave person

MODULES USED

- Route discovery
- Detecting attacks
- Implementation of path tracing algorithm

MODULE DESCRIPTION

(1). Route Discovery and Transfer

AODV algorithm is made use here. The 3 methods are RREQ, RREP, RERR. With the Acknowledgement gained AODV finds the right path with Shortest Distance. It takes into account only the nearby node. It transfers the packet to that discovered Node.

(2). Detecting Attacks

Many attacks like selfish, stretched, misbehaviour, black hole. By Making use of specific threshold values that

(3).Implementation of Path Tracing Algorithm

It makes use of a Dummy message to check the availability of a node and gain acknowledgement.

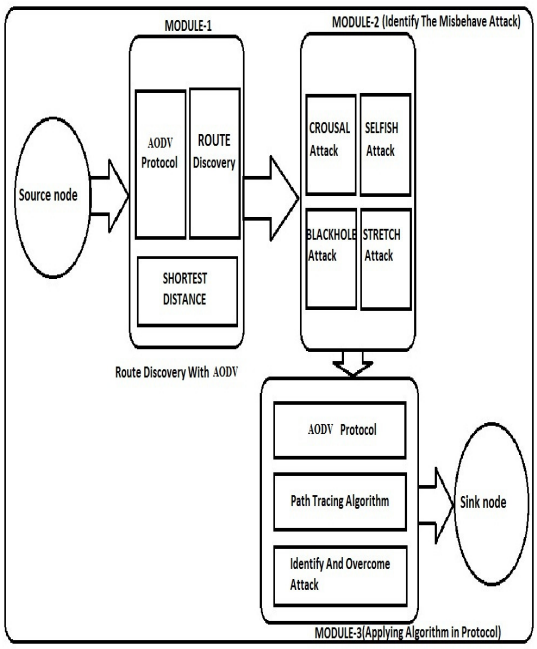
- It has few or more steps to implement:
- Route discovery
- Compute per hop distance using RTT
- Compare per hop distance with prior per hop distance
- Check IF DBC-DAB> RTh
- Check number of times the link participates in the path
- IF FAcount> FATh
- Broadcast data packet
- Malicious node detected & isolated from network

are predefined, the malicious nodes can be detected easily

ARCHITECTURE DIAGRAM

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018



WORKING OF AODV PROTOCOL

By using the AODV protocol we can discover the route which is nearby.If an AODV router receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields:

• Destination address

• Next hop address

• Destination sequence number

• Hop count

If a route exists, the router simply forwards the message to the next hop. Else, it saves the message in a message queue, and then it initiates a route request to determine a route

AODV PROPERTIES

AODV discovers routes as and when necessary. Does • not maintain routes from very node to every other.Routes are maintained just as long as necessary. Every node maintains its monotonically increasing.sequence number increases every time the nodenotices change in the neighbourhood topology. AODVutilizes routing tables to store routing informationA Routing table for unicast routes A Routing table for multicast routes. The route table stores:<destination addr, next-hop addr,destination sequence number, life time> For each destination, a node maintains a list of precursor nodes, to routethrough them Precursor nodes help in route maintenance (more later).Life-time updated every time the routeis used. If route not used within its life time -> it expires.

IV.PATH TRACING ALGORITHM

It has two stages.

Stage 1:

The source hub surges the course asks for (RREQ) bundlesthrough prompt neighbors towards end. When it achievesthe end, it sends back course answer (RREP) in the opposite way. The way subtle elements are put away in the DSRsteering store. Keeping in mind the end goal to recognizethe wormhole, we advance the general DSR header byincluding additional fields. Former every jump separationfield, every bounce separation field and timestamp fields are added to the header of every bundle. Consider bothformer every jump separation and every bounce remove inorder to look at the contrast between the two separations.In the event that the distinction is excessively expansivethat surpasses the most extreme edge esteem, then wormhole is distinguished. All hubs that partake in the directing instrument perform this operation. The timestamp field is introduced to the time of the first bit of RREQ is sent. Every jump separation field can be changed by middle person hubs however timestamp field can't be modified by whatever other hubs. At whatever point a middle person hub acquires RREQ, it figures every jump separation with its prompt neighbor and contrasts it and the former every bounce remove in the header esteem. After the correlation, it puts every bounce separate in the earlier every jump separation field in the bundle header and advances RREQ to its neighboring hubs. On getting RREQ, the collector figures every bounce separation with its neighbor in the converse way and it puts in the bundle header. Each middle hub advances one RREP for every RREQ. Each RREP holds the every jump separation of all way in which it is connected. Not withstanding every jump separation esteem, it likewise holds the timestamp of the time when taken in the middle of sending and getting the RREQ and RREP correspondingly between two hubs. The calculation of every bounce separation of every hub is clarified in the following segment.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Every Hop Distance Estimation

The vicinity of wormhole can be recognized by computing the separation between each one bounce in a way consider Round Excursion Time (RTT) worth to figure the every jump separation. RTT is characterized as RREQ and RREP spread time between the source and objective. Given us a chance to consider the RTT count between two hubs A and B where both the hubs are non-wormhole.

Variables used in RTT Calculation

Prep: Time when the first bit of RREP is received from B.

Qreq: Time when the last bit of RREQ is broadcasted to A.IPD: Intra nodal processing delay The RTT between two nodes are calculated by using formula

(1) ΔT= RTT= Prep – Qreq – IPD (1)

With the estimated value of ΔT, per hop distance between X and Y 'ZXY' is calculated assuming that routing signals travel with the speed of light 'v'.ZXY = (v /2) ∗ΔT

(2) The node verifies whether B resides within its maximum acceptable transmission range RT. v is a constant and it has the value of 3×10–8 ms–1. The value of RTT is in the order of micro seconds and transmission range is in the order of a meter. In the same way per hop space between node Y and node Z, ZYW is calculated where X, Y, and Z are consecutive neighbors of a path. The node C considers ZXY as the prior per hop distance and compares with ZXY. If the difference between ZXY and ZYX is larger than the maximum threshold range, Rth then the link with higher per hop distance is said to be wormhole. ZYX - ZXY>Rth.

(3) The calculation of per hop distance is performed during the route discovery process in order to reduce the routing overload.

Each node must run the per hop distance calculation using RTT value and store the estimated per hop distance value in packet header. The wormhole can be detected using the information in the packet header.

Stage 2

1. Each node in the network has to perform four major operations to detect the wormhole attack.

2. Compute per hop distance and compare it with the prior per hop distance.

3. Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value.

4. If it is larger, then the wormhole is detected and it is informed to all other nodes in the networks to provide wormhole alertness.

5. For the confirmation of wormhole attack, the number of time a link is used in a path is also checked in addition to comparison of per hop distance.

If ZYW - ZYX> Rth and DA count > DA_{th} then it is a wormhole link. Every per hop separation is ascertained at the time of course disclosure to make our proposal vitality proficient. Numerous courses are found from figure every per hop separation and stores in the parcel header. By looking at the every per hop separate between all hubs in a way, a wormhole can be identified. In the event that the every per hop separation surpasses the earlier every per hop separate through a most extreme edge range Rth, then the way identified with that specific hub is wormhole. For the compelling wormhole discovery, we take an alternate parameter called continuous appearance.

Steps for Path Tracing Algorithm

Steps to locate the wormhole assaults

.Step 1: Nodes in a way figures RTT qualities focusedaround the time between the RREQ sent and RREP got.The RTT reckoning is focused around its own clock.

Step 2: Compute every jump separation worth utilizingRTT esteem. The figured every bounce separation worthand timestamp are put away in every bundle header.

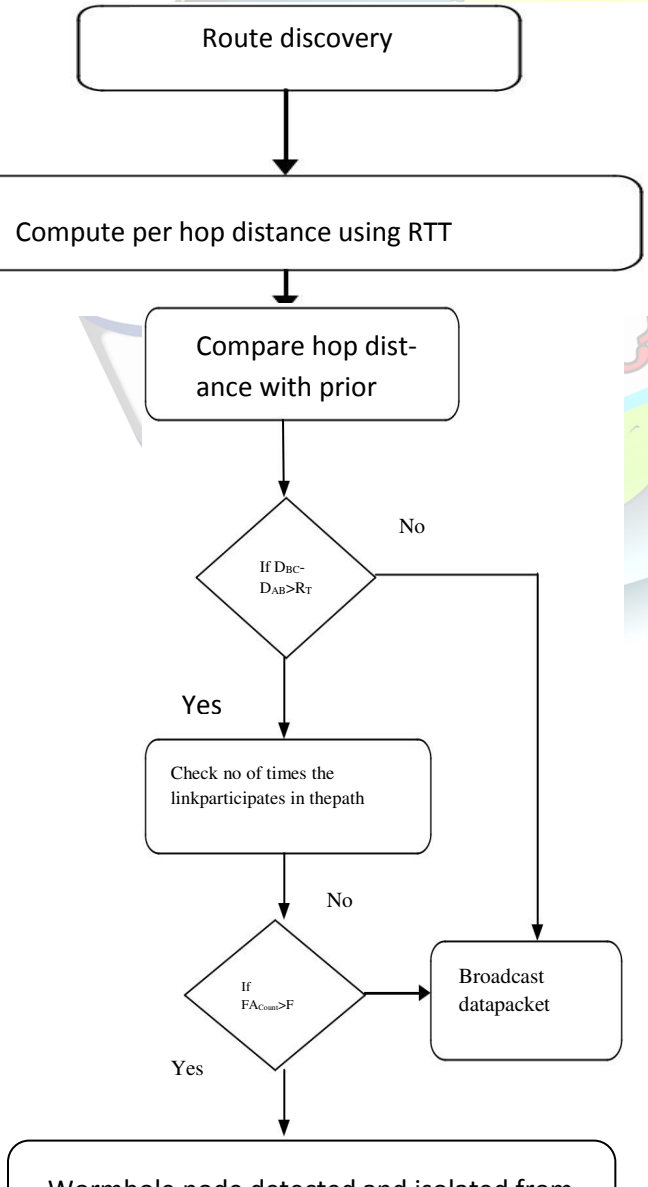
Step 3: These information's are put away to distinguish thewormhole join. Each hub in a way registers every jump separation with its neighbor and contrasts it and the former every bounce separation. In the event that the everybounceseparation surpasses the greatest limit range, Rth ,go to Step 4.

Step 4: Check for the greatest include a connection partakes the way. On the off chance that FA count >Fth, thenthe connection is wormhole.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Step 5: Mark the connection as wormhole and the relatinghub educates different hubs to caution the system. Thesewormhole hubs are then separated from the system appearance.Of the packet will be more increasingly higher for8.6the red line that is with attacker than that of the green line whi-ch is attacker-multisec.The packet-loss for the attack by the type with attackeris about 81.5% which is a highamo- unt of loss that isalmost most of the packet will be lost in this type.



ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

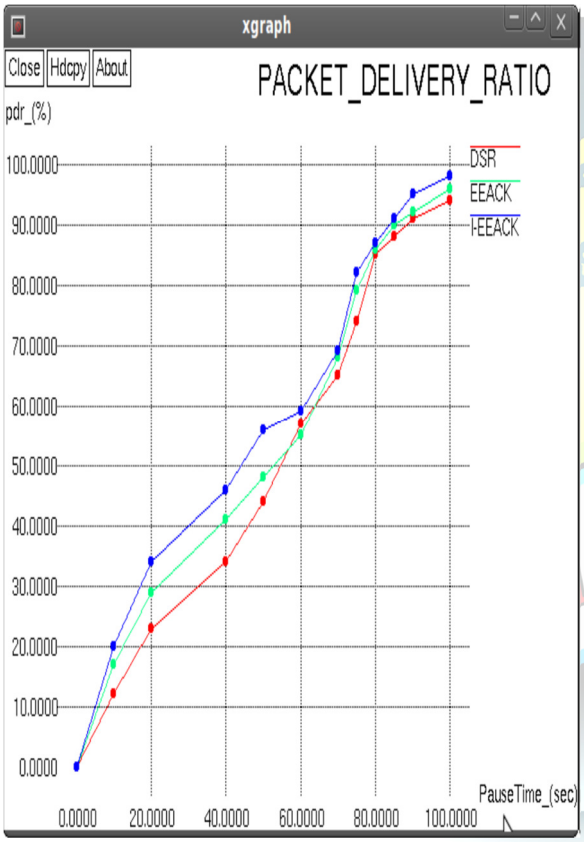
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

PERFORMANCEEVALUATION

The metrics used in evaluating the performance are:

(1) Packet Delivery Ratio

It is the ratio of the number of data packets delivered to the destinations to the number of data packets generatedby the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence ofmalicious nodes. It can be defined as: PDR = total no.of packet received / total no. of packet send.

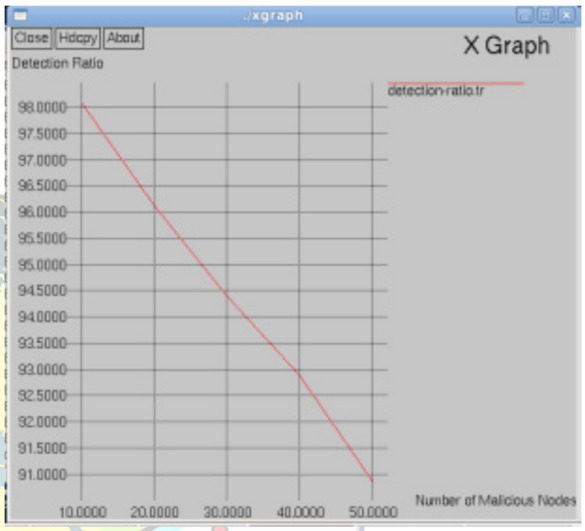


(2). Detection Ratio

DetectionRatio = NoofMaliciousNodes Detected

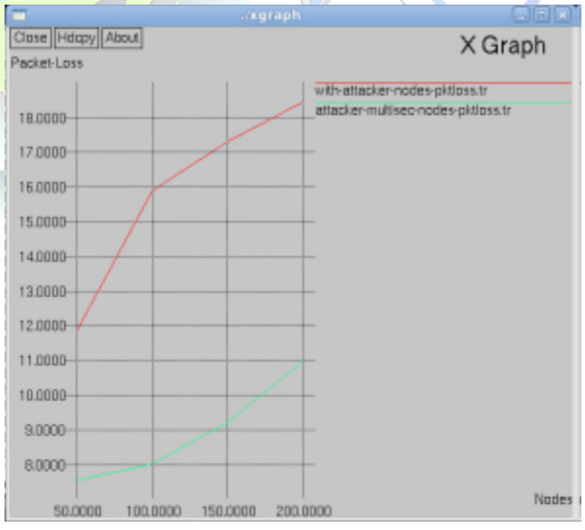
No of Malicious Node.

The above graph represent the detection ratio of the malicious node which is been detected by the simulator. The number of malicious node is been estimated to 50 and the ratio of the detection is been mentioned above. The red line represents the detection ratio line representation. This is the detection ratio graph for the warm hole attackdetection using path tracing method using AODV protocol it is nothing but on-demand distance vector. The total number of nodesused in this experiment is 200nodesandthe number of malicious node is kept to be as 50.The detection ratio graph decreases as the node move to the final node.



(3). Packet Loss

It represent the packet-loss which is nothing but the amount of packets which is been dropped while the attack is been implemented. The comparison of the packet loss between different attack is been mentioned in the figure the red line will be representing the with-attacker and the green line will be representing the attacker-multisec. The losses



ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Of the packet will be more increasingly higher for8.6the red line that is with attacker than that of the green line which is attacker-multisec.The packet-loss for the attack by the type with attackeris about 81.5% which is a highamount of loss that isalmost most of the packet will be lost in this type. The attack multisec the amount of packet-loss will beabout 44.85% which is low in comparison with the redline.Packet Delivery Ratio, Average delay, Packet-loss,Detection-ratio compare than other wormhole attacks.This approach will help wireless ad-hoc networks toimprove security.

(4). Average Delay

The Average Delay is the elapsed time between the pa-cket sent and received. Attack increase the End to End delay (shown in Red) and the proposed method significa-ntly reduce the End to End delay by avoiding the Attacker (shown in Green); Graph describes the dependence of the End to End delay on the number of nodes in action. All path increases with increasing the number of nodes inthe network. But defence path are decrease compare than attacker path for reduce the delay.Here some selected analysis node (50, 100, 150 and 200) results are available from simulation with two routes. First route is with Attacker path with malicious node in Red col-or. Second route is Defence path, where malicious nodes are isolated in green color.

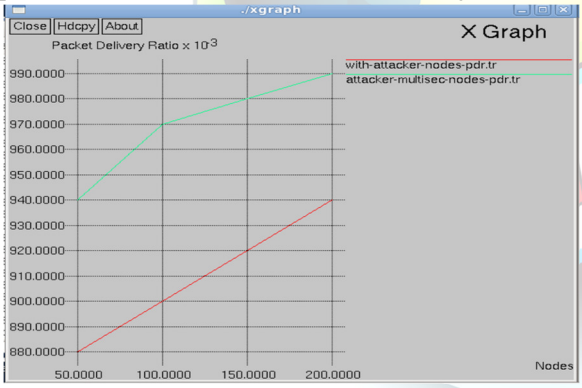


Fig shows the End to End delay of two different routes as AODV, Attacker on AODV and Defence mechanism on Attack based AODV. In that X-axis specifies the node and Y-axis specifies the Average Delay. Here we compare two Routes for average delay with the proposed method. When maliciousnode occurrence is 0 then this method givereduce average delay. Average at node 200 in increment order. When malicious node are occur in this normal path then it is called With Attacker path (in the red) is providing 45.9 percent average delay at node 200 in increment order and when malicious node are isolated then it is calledAttacker multisec (in the Green) is providing 20% packet delivery ratio at node 200 in increment order but attacker multisec are decrease and providing reduce delay compare than attacker path.

V.CONCLUSION

Mobile ad hoc networks (MANET) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. AODV protocol itself incurs a low checking overhead. However, to prevent malicious users from providing fake data transmission, calculate the dropping and losing packet size, packet delivery ratio for optimal estimation. Here we implementing and finding thedropping packets for optimal estimation for AODV. Path tracing algorithm to detect the malicious attack using per hop distance and pixel wise measurements link frequent appearance count parameters using AODV. So we can detect accurate misbehave person. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

REFERENCES

[1] Ayday,.E Lee,.H and Fekri,.F(2010)"Trust Management and Adversary Detection for Delay-Tolerant Networks,"Proc. Military Comm.Conf.(Milcom '10).

[2] Burgess,.JGallagher,.BJensen,.D and Levine,.B(2006) "Maxprop : Routing for Vehicle-Based Disruption-Tolerant Networks," Proc.IEEE INFOCOM '06.

[3] Chen.B.B and Chan,.M.C "Mobicent(2010): A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM '10.

[4] Douceur,.J (2001)"The Sybil Attack," Proc. Revised Papers from the First Int'l Workshop Peer-to-Peer Systems (IPTPS '01).

[5] Fudenberg,.F.D and Tirole,.J(1991) Game Theory. MIT Press.

[6] Gao.W and Cao,.G(2011) "User-Centric Data Dissemination in

[7] Disruption-Tolerant Networks," Proc. IEEE INFOCOM '11.

[8] Hossmann,.T Spyropoulos,.T and Legendre,.F(2010) "Know the Neighbor:

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEEINFOCOM '10.

[9] Keranen,.A Ott,.J and Karkkainen,.T(2009) "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf.Simulation Tools and Techniques (SIMUTools '09).

[10] Lindgren.A and Doria,.A(2007) "Probabilistic Routing Protocol for Intermittently Connected Networks,"draft-lindgren-dtnrg-prophet-03.

[11] Li,.FSrinivasan,.A and Wu,.J(2009) "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc.IEEE INFOCOM '09.

[12] Li,.QZhu,.S and Cao,.G(2010) "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10.