Indian Journal of Science and Technology, Vol 8(17), DOI: 10.17485/ijst/2015/v8i17/63541, August 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Performance Metrics of Wormhole Detection using Path Tracing Algorithm

M. Reji*, P. C. Kishore Raja, Christeena Joseph and Radhika Baskar

Electronics and Communication Engineering Department, Saveetha University, Chennai - 600072, Tamil Nadu, India;
rejime@gmail.com, pckishoreraja@gmail.com, Christeena003@gmail.com, radhikabaskr@gmail.com

Abstract

Objective: Mobile Adhoc Networks contains set of mobile nodes does not have a fixed structure. It is very important to protect the network secure. The main aim of the paper is to protect the network from worm hole attack using path tracing algorithm with the advancement of aodv and compare the performance parameters. **Methods:** We propose path tracing algorithm for detection of worm hole attack as a extension of aodv protocols the path of the node effectively computes the per hop distance of its neighbor node with per hop distance of the previous node to identify the worm hole attack. NS2 simulator is used to compare the performance parameters of the worm hole attack. **Conclusions:** Simulated parameters like packet delivery ratio, delay, and packet loss with attacker and without attacker are done and the detection ratio is identified.

Keywords: AODV Protocols, Mobile Adhoc Network, Path Tracing, Worm Hole Attack

1. Introduction

For dispatching a wormhole assault, an enemy interfaces two far off focuses in the system utilizing an immediate low-inertness correspondence connection called as the wormhole join. The wormhole connection could be built by a mixture of means, e.g., by utilizing an Ethernet link, a long-go remote transmission, or an optical connection. Once the wormhole connection is made, the foe catches remote transmissions toward one side, sends them through the wormhole connect and replays them at the flip side. Here X and Y are the two end-purposes of the wormhole connection (called as wormholes). X replays in its neighbourhood (in region An) everything that Y hears in its own particular neighbourhood (territory B) and the other way around. The net impact of such an assault is, to the point that all the hubs in range An expect that hubs in zone B are their neighbours and the other way around. This, therefore, influences directing and other network based conventions in the system. Once the new courses are secured and the movement in the system begins utilizing the X-Y alternate way, the wormhole hubs can begin dropping parcels and reason system interruption. They can likewise spy on the parcels experiencing and utilize the vast measure of gathered data to break any system security. The wormhole assault will additionally influence integration based confinement calculations and conventions focused around restriction, in the same way as geographic steering, will discover numerous inconsistencies bringing about further system disturbance.

2. Overview of Attacks in Manet

2.1 Assaults against Adhoc Networks

While a remote framework is more adaptable than a wired one, it is in like manner all the more vulnerable against strikes. This is a direct result of the very nature of radio transmissions, which are set aside a few minutes. On a wired framework, an interloper would need to break into a machine of the framework or to physically wiretap a connection. On a remote framework, an adversary can listen stealthily on all messages inside the release zone, by meeting

*Author for correspondence

expectations in random mode and using a package sniffer (and conceivably a directional gathering mechanical assembly). Thus, by fundamentally being inside radio expand, the interloper has permission to the framework and can without a doubt catch transmitted data without the sender really knowing (for instance, imagine a Portable machine a vehicle ceased in the city keeping an eye on the correspondences inside a nearby by building). As the gatecrasher is perhaps indistinct, it can furthermore record, adjust, and after that retransmit distributes they are emitted by the sender, really envisioning that packages begin from a genuine social affair. Furthermore, on account of the breaking points of the medium, exchanges can without a doubt be irritated; the intruder can perform this ambush by keeping the medium discovered up with sending its own specific messages, or just by staying correspondences with confusion.

2.2 Assaults against the Steering Layer in Manets

We now concentrate on assaults against the directing convention in impromptu systems. These assaults may have the point of changing the directing convention so activity courses through a particular hub controlled by the aggressor. An assault might likewise go for hindering the arrangement of the system, making genuine hubs store inaccurate courses, and all the for the most part at annoying the system topology. Assaults at the steering level can be arranged into two primary classes: mistaken activity era and wrong movement handing-off. Now and again these agree with hub misbehaviors that are not because of malevolence, e.g. hub glitch, battery weariness, or radio obstruction.

2.3 Replay Attack

As topology changes, old control messages, however substantial previously, portray a topology arrangement that no more exists. An aggressor can perform a replay assault by recording old legitimate control messages and re-sending them, to make different hubs upgrade their directing tables with stale courses. This assault is effective regardless of the possibility that control messages bear an overview or a computerized mark that does exclude a timestamp.

2.4 Wormhole Attack

The wormhole assault is truly extreme, and comprises in recording activity from one district of the system and replaying it in an alternate area. It is completed by an interloper hub X found inside transmission scope of true blue hubs A and B, where A and B are not themselves inside transmission scope of one another. Gatecrasher hub X just shafts control movement in the middle of A and B (and the other way around), without the alteration assumed by the steering convention – e.g. without expressing its address as the source in the bundles header – with the goal that X is essentially imperceptible. This result in an unessential inexistent A - B join which indeed is controlled by X, Node X can a short time later drop burrowed parcels or break this connection without restraint. Two interloper hubs X and X′, joined by a remote or wired private medium, can likewise intrigue to make a more extended (and more destructive) wormhole. The seriousness of the wormhole assault originates from the way that it is hard to locate, and is successful even in a system where classifiedness, uprightness, validation and non-denial (by means of encryption, processing, and advanced mark) are saved. Besides, on a separation vector steering convention, wormholes are prone to be picked as courses in light of the fact that they give a shorter way – though bargained – to the goal. Marshall brings up a comparative assault, called the imperceptible.

2.5 Black Hole Attack

On the off chance that a hub neglects to transfer TC messages, the system may encounter network issues. In systems where no repetition exists (e.g. in a strip), integration misfortune will without a doubt result, while different topologies may give excess network. On the off chance that MID and HNA messages are not legitimately hate, extra data in regards to different hubs interfaces and associations with outer systems may be lost.

3. Related Work

Reputation based plans recognize the malevolent hub and tell different hubs about the getting into mischief node[1]. This plan is focused around the essential of rebuffing the hubs by blocking vindictive hub perpetually from the network[2]. Impetus based methodologies expect to advance positive conduct as opposed to reporting and punishing misbehaving hubs[3,4]. This plan is focused around the essential to distinguish the trust level of hub and advances the node which is more trusted[5–7] have created a circulated and helpful Interruption Location Framework (IDS) where individual IDS operators are set on every single hub. Every IDS specialists runs autonomously, discovers intrusion from nearby follows and launchs response,

bhargava and Agrawal[9] have amplified the IDS model portrayed in[10]] to improve the security in Adhocon Demand Distance Vector (AODV) steering convention. Guard dog[11], proposes to screen parcel forwarding, and has the confinement to depend on catching of bundle transmissions for neighbouring hubs for location of inconsistencies in bundle sending. Kong J[8], takes after the idea of guard dog yet meets expectations with ADOV. It includes a next jump field in AODV bundles so that a hub can be mindful of the right next bounce of its neighbours and considered more sorts of assaults, for example, parcel alteration, bundle duplication, and bundle sticking, Dosattacks. Bal Krishnan[12] has proposed an approach to locate bundle dropping in Adhoc systems. There are various research is done in the bearing in which analyst utilized the trust emphasizes as a part of existing trust based routing schemes for Adhoc system.[7,13–17,] are based upon the trust based discovery schemes for Manet Razak, et al.[13], examined the issues in regards to the interloper and security of Adhoc system, alongside the discussion of the current examination lives up to expectations they proposed a model to secure MANET. In the wake of considering these issues, a novel however the theoretical IDS system is proposed to enhance the performance of existing IDS in MANET environment. They proposed the model for peculiarity location and misuse recognition on the premise of mark based and fellowship based identification mechanism Abusalah et al.[14], proposed a Trust Aware Routing Protocol (TARP) for secure trusted Adhoc steering. Intarp, security is naturally incorporated with the steering convention where every hub assesses the trust level of its neighbours focused around a set of traits. Covering, is not an interruption recognition system pirzada et al.[15], depicts that reliance on a focal trust power is an unrealistic prerequisite of Adhoc system. They displayed a model for trust based correspondence in Adhoc systems. The model introduced the idea of conviction and gives an element measure of dependability and reliability focused around direct trust system in an Adhoc system. They quantized the trust for distinctive trust bunches lastly compute the trust to separate in the middle of malevolent and trusted node yan et al.[17], utilized the trust assessment based security answer for portable Adhoc organize yet it is best suited for notoriety based schemes Eschenauer et al.[16], exhibited a skeleton for trust foundation that backings the prerequisites for manets and depends on distributed record imparting for confirmation appropriation through the system.[18] They describe that issue of confirmation circulation for trust foundation is to a degree not the same as the ordinary record sharing problem in shared systems. Consequently, they proposed to utilize a swarm insights approach for the outline of trust confirmation appropriation rather than basically depending on a conventional distributed record offering system[19,20]. They likewise contended that the configuration of measurements for the assessment of trust proof is a vital part of trust establishment in Manets. Though Reputation based plans are great if there should be an occurrence of wired system or where there is idea of focal power or some observing focuses, yet these calculations/models are fizzling when we connected them to the portable Adhoc environment. Because of issues like no focal power and self-configurable system and highly dynamic topology with a high level of versatility makes extremely hard to outline an impeccable interruption detection system for versatile Adhoc system. One of the primary issues in MANET IDS is on the quantity of false alarms raised on the system as an aftereffect of false claims/reports made by individual hubs[23–25]. This secrecy issue is abig challenge in Adhoc system on the grounds that it is troublesome for hubs to recognize trusted and maliciousnodes in such self-sufficient systems[26]. Black hole attack can be identified using ip address in mobile adhoc networks[21,22].

4. Proposed Work

4.1 Path Tracing Method

Our proposal includes two stages. All sending hubs process every bounce separation and time in phase and in stage 2 all hubs catches the vicinity of wormhole utilizing the data assembled as a part of stage 1.

Stage 1

The source hub surges the course asks for (RREQ) bundles through prompt neighbors towards end. When it achieves the end, it sends back course answer (RREP) in the opposite way. The way subtle elements are put away in the DSR steering store. Keeping in mind the end goal to recognize the wormhole, we advance the general DSR header by including additional fields. Former every jump separation field, every bounce separation field and timestamp fields are added to the header of every bundle. We consider both former every jump separation and every bounce remove in order to look at the contrast between the two separations. In the event that the distinction is excessively expansive that 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.

4.2 Every Hop Distance Estimation

The vicinity of wormhole can be recognized by computing the separation between each one bounce in a way We 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 An and B where both the hubs are non-wormhole.

4.3 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) $\Delta T = RTT = Prep - Qreq - IPD$ (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 neighbours 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 > DAth 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 the course disclosure process. All hubs in every way 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 R^{th}, then the way identified with that specific hub is wormhole. For the compelling wormhole discovery, we take an alternate parameter called continuous appearance.

5. Path Tracing Algorithm

Steps to locate the wormhole assaults.

Step 1: Nodes in a way figures RTT qualities focused around 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 utilizing RTT esteem. The figured every bounce separation worth and timestamp are put away in every bundle header.

Step 3: These information's are put away to distinguish the wormhole join. Each hub in a way registers every jump separation with its neighbour and contrasts it and the former every bounce separation. In the event that the every bounce separation surpasses the greatest limit range, R^{th} , go to Step 4.

Step 4: Check for the greatest include a connection partakes the way. On the off chance that FA count $>F^{th}$, then the connection is wormhole.

Step 5: Mark the connection as wormhole and the relating hub educates different hubs to caution the system. These wormhole hubs are then separated from the system.

5.1 AODV Protocol

Our essential proposal could be known as an unadulterated on interest course procurement framework hubs that don't lie on dynamic ways none, of these keep up any directing data nor take part in any intermittent steering table trades. Further a hub does not need to find and keep up a course to an alternate hub until the two need to impart unless the previous hub is ordering its administrations as a moderate sending station to keep up network between two different hubs. When the neighborhood integration of the portable hub is of investment every versatile hub can get to be mindful of alternate hubs in its neighbourhood by the utilization of a few methods including nearby not system wide telecasts known as hi messages. The steering tables of the hubs inside the area are sorted out to enhance reaction time to neighborhood developments and give fast reaction time to demands for foundation of new courses. The calculations essential goals are to show revelation bundles just when fundamental. To recognize nearby network administration neighborhood identification and general topology support. To spread data about progressions in neighborhood network to those neighboring versatile hubs that is prone to need the data.

- AODV utilizes a telecast course disclosure component as is additionally utilized with modifications within the Dynamic Source Routing DSR calculation.
- Instead of source directing however AODV depends on rapidly making course table entrances at halfway hubs. This distinction pays off in systems with numerous hubs where a bigger overhead is brought about via convey source courses in every information parcel. To keep up the latest steering data between hubs we obtain the idea of end of the line arrangement numbers from DSDV.
- Unlike in DSDV however every adhoc hub keeps up a monotonically expanding grouping number counter which is utilized to supersede stale stored courses The mix of these methods yields a calculation that uses data transmission efficiently by minimizing the system load for control and information activity is receptive to changes in topology and guarantees loop free site.

5.2 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 node notices change in the neighbourhood topology. AODV utilizes routing tables to store routing information
- A 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 route through them Precursor nodes help in route maintenance (more later). Life-time updated every time the route is used If route not used within its life time -> it expires.

6. Implementation

The simulation study is performed using the NS-2 VERSION 2.34 simulator. Performance of PT algorithm is analyzed and graph is depicted in the presence of 50 nodes including malevolent nodes and target. The routing protocol used for simulation is AODV. The nodes adopt a CBR traffic pattern for communication. The simulation parameters are shown in the Table 1.

7. Performance Metrics

7.1 Packet Delivery Ratio

PDR is the proportion of the total amount of packets reached the receiver and amount of packet sent by the source. If the amount of malicious node increases, PDR also decreases gradually. The higher mobility of nodes causes PDR to decrease.

$$PDR = \frac{\text{Total amount of data packet Received (Receiver)}}{\text{Total amount of packet Sent (Source)}}$$

Attack reduces the average packet delivery Ratio (shown in the Red) and the proposed method significantly regains the packet delivery Ratio by avoiding the attacker (Shown in green) Figure 1 describes the dependence of the packet delivery ratio on the number of the nodes in action. All path decreases with increasing the number of nodes in the network but defence path are increase compare than attacker path.

Here it shows some selected analysis node (60, 80, 100, 120, 140, 160, 180 and 200) results are available from the simulation with two routes. First route is With attacker without malicious node in Red colour. Second route is Attacker with multispeed seconds defence path where malicious nodes are isolated in green colour.

Table 1. Simulated Parameters

FEATURES	DESCRIPTIONS
Simulator	NS-2 version 2.34
Mobility model	Path Tracing Method
Routing protocol	AODV
Tunnel length	50 node
Number of nodes	200
Simulator area(mxm)	600*600
Simulation time	120seconds
Transmission rate	250m
Packet sending rate	100 pkt/sec
Nodes in all scenarios	50,100,150,200
Traffic Type	CBR
MAC	802.11
Packet size	512 byte
Performance Parameters	PDR, Detection ratio, and Average Delay
Examined approaches	Normal, Attack and Defence

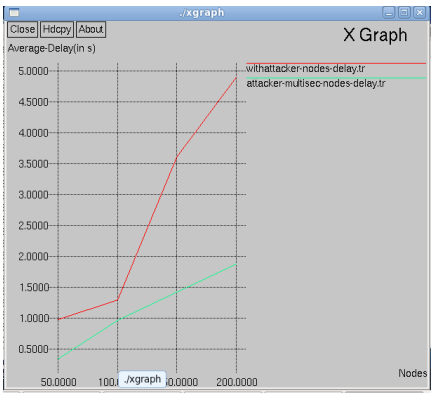
Table 2. Packet Delivery Ratio with Attacker and Without Attacker

Node	With Attacker In percentage	Attacker Multi second Node
50	88.5	0.945
100	89.2	0.959
150	90.0	0.970
200	90.8	0.947

Graph 1 shows the Packet Delivery Ratio of two different routes as AODV, Attacker on AODV and Defence Mechanism on Attack based AODV. In that X-axis specifies the packet delivery ratio. Here we compare two routes for packet delivery ratio with the proposed method give a good packet delivery ratio. When malicious node are occur in path then it is called With Attacker Path (in the red) is providing 72.9% packet delivery ratio at node 200 in decrement order and when malicious node are isolated then it is called Attacker multisec path (in the green) is providing 77.8% packet delivery ratio at node 200 in decrement order. But defence path are increase and provide better packet delivery ratio compare than with attacker path.

7.2 Average Delay

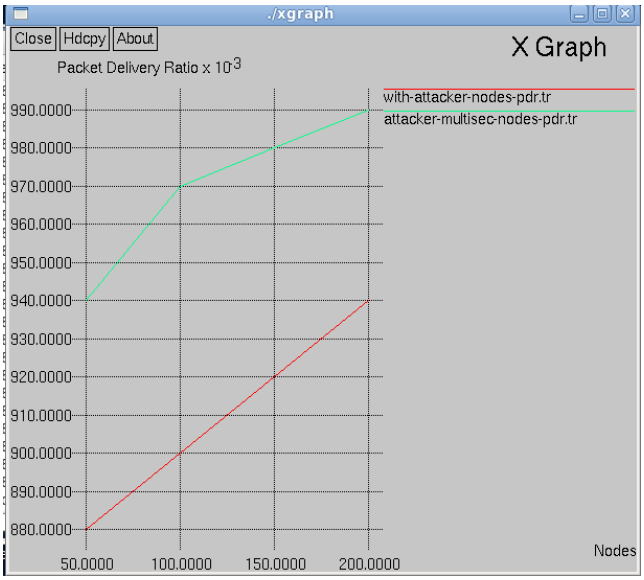
The Average Delay is the elapsed time between the packet sent and received. Attack increase the End to End delay (shown in Red) and the proposed method significantly reduce the End to End delay by avoiding the Attacker (shown in Green); Graph 2 describes the dependence of the End to End delay on the number of nodes in action. All path increases with increasing the number of nodes in



Graph 1. PDR for 50 and 100 nodes.

the network. But defence path are decrease compare than attacker path for reduce the delay.

Here in Table 3, 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 colour. Second route is Defence path, where malicious nodes are isolated in green colour. 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 malicious node occurrence is 0 then this method give reduce 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 called Attacker 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.



Graph 2. Average Delay.

Table 3. Average Delay with Attacker and Without Attacker

NODE	WITH ATTACKER In Percentage	ATTACKER MULTISEC
50	1.1000	0.4900
100	1.2000	0.7500
150	1.3000	0.9900
200	2.2500	1.2000

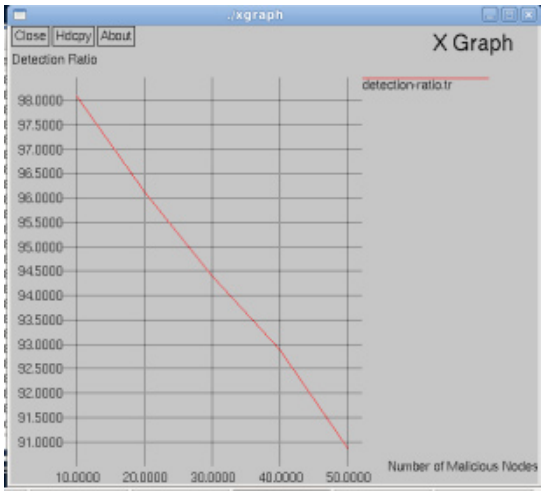
7.3 Detection Ratio

$$\text{Detection Ratio} = \frac{\text{No of Malicious Nodes Detected}}{\text{No of Malicious nodes}}$$

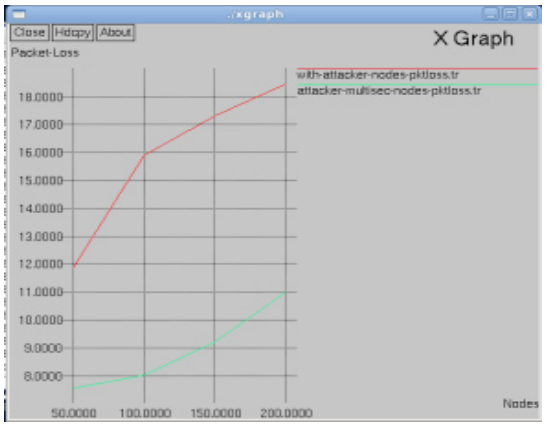
The above graph represent the detection ratio of the malicious node which is been detected by the simulator. The number of malicious node is been estimated to 50 and the ratio of the detection is been mentioned above. The red line represents the detection ratio line representation. This is the detection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

7.4 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 of the packet will be more increasingly higher for



Graph 3. Detection Ratio.



Graph 4. Packet Loss.

Table 4. Packet Loss with Attacker and Without Attacker

NODE	WITH ATTACKER	ATTACKER MULTISEC
50	12.7	7.7
100	14.3	7.9
150	15.9	8.1
200	16.5	8.6

the 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 attacker is about 81.5% which is a high amount of loss that is almost most of the packet will be lost in this type. Then in the attack multisec the amount of packet-loss will be about 44.85% which is low in comparison with the red line.

Packet Delivery Ratio, Average delay, Packet-loss, Detection-ratio compare than other wormhole attacks. This approach will help wireless ad-hoc networks to improve security.

8. Conclusion

There have been numerous examination to overcome worm gap assaults in specially appointed systems by security structural engineering, framework or administration, for example, authentication, encryption, additional fittings support and so forth. In this paper we exhibit a technique by way discovery which is focused around AODV utilizing recreations created within Network Simulator to shield again the worm gap assault in remote impromptu systems and here wormhole assault is caught without any fittings, area data and clock synchronization. Distinguish wormhole hub and avoid them. At last enhance Packet Delivery Ratio, Average postponement, Packet-misfortune, Detection-degree think about than other wormhole assaults. These methodologies will help remote ad-hoc systems to enhance security.

8. References

1. Wan Z, Kui R, Ming GU. USOR: An unobservable secure on-demand routing protocol for mobile ad hoc networks. 2012 May; 1(5):1922–32.
2. Pfitzmann A, Hansen M. Anonymity, unobservability and pseudonymity: A consolidated proposal for terminology. Draft; 2000 Jul.
3. Zhu Y, Fu X, Graham B, Bettati R, Zhao W. On flow correlation attacks and counter measures in mix networks. PET04, LNCS 3424; 2005. p. 207–25.
4. Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM. 1981 Feb; 4(2):84–90.
5. Otrok H, Debbabi M, Assi C, Bhattacharya P. A cooperative approach for analyzing intrusions in mobile ad hoc networks. 27th International Conference of Distributed Computing Systems Workshops (ICDCSW '07); 2007 Jun 22–29. p. 86. DOI: 10.1109/ICDCSW.2007.91.
6. Davis J, Hill E, Spradley L, Wright M, Scherer W, Zhang, Y. Network security monitoring - intrusion detection. 2003 IEEE of Systems and Information Engineering Design Symposium. 2003 Apr; 241(246):24–5. DOI: 10.1109/SIEDS.2003.158030.
7. Yan Z, Zhang P, Virtanen T. Trust evaluation based security solution in ad hoc networks. Proceedings of the 7th Nordic Workshop on Secure IT Systems. Gjovik, Norway: NordSec; 2003. p. 1–14.
8. Kong J, Petros Z, Luo H, Lu S, Zhang L. Providing robust and ubiquitous security support for mobile ad-hoc net-works. Ninth International Conference on Network Protocols; 2001 Nov 14. p. 251–60. DOI: 10.1109/ICNP.2001.992905.
9. Bhargava S, Agrawal DP. Security enhancements in AODV protocol for wireless ad hoc networks. 54th IEEE Vehicular Technology Conference (VTC, VTS 2001); 2001. p. 2143–7. DOI: 10.1109/VTC.2001.957123.
10. Zhang Y, Lee W. Intrusion detec¬tion in wireless ad-hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00). New York, NY, USA: ACM; 2000. p. 275–83. DOI: 10.1145/345910.345958.
11. Chengqi S, Zang Q. Suppressing selfish behavior in Adhoc networks with one more hop. 5th International ICST Conference on Heterogeneous Networking for Quality,

Reliability, Security and Robustness. Lecture Notes in Mobile Networks and Applications, Computer Science; Netherlands: Springer; 2009 Apr 1. p. 178–87. ISBN: 978-963-9799-26-4. DOI: 10.1007/s11036-008-0145-2.
12. Balakrishnan K, Jing D, Varshney V K, TWOACK: Preventing selfishness in mobile ad hoc networks. IEEE Wireless Communications and Networking Conference; 2005 Mar 13–17. p. 213742. DOI: 10.1109/WCNC.2005.1424848.
13. Razak SA, Furnell S, Clarke N, Brooke P, Mehrotra S. Zeng D, Chen H. Thuraisingham B. A TwoTier Intrusion detection system for mobile ad hoc networks - A friend approach. Lecture Notes in Computer Science. Berlin/Heidelberg: Springer. 2006; 3975:590–5. DOI: 10.1007/11760146.
14. Abusalah L, Khokhar A, Guizani M. NIS01-4: Trust aware routing in mobile ad hoc networks. IEEE Global Telecommunications Conference (GLOBE COM '06); 2006 Dec 1. p. 1–5. DOI: 10.1109/GLOCOM.2006.264.
15. Pirzada AA, McDonald C. Establishing trust in pure ad-hoc networks. Proceedings of the 27th Australasian Computer Science Conference (ACSC'04); Dunedin, New Zealand. 2004. p. 47–54.
16. Eschenauer L. On trust establishment in mobile ad-hoc networks [Master's Thesis]. Department of Electrical and Computer Engineering, University of Maryland; 2002.
17. Zouridaki C, Brian L, Mark, Hejmo M, Thomas RK. E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks. Ad Hoc Networks. 2009 Aug; 7(6):1156–68. ISSN: 1570-8705. DOI: 10.1016/j.Adhoc.2008.10.003.
18. Yi-An H, Lee W. A cooperative intrusion detection system for ad hoc networks. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN'03). New York, NY, USA: ACM; 2003. p. 135–47. DOI: 10.1145/986858.986877.
19. Capkun S, Buttyan L, Hubaux J. Self organized public-key management for mobile ad hoc networks. IEEE Trans Mobile Comput. 2003 Mar; 2(1):52–64.
20. Kong J, Hong X. ANODR: Aonymous On Demand Routing with untraceable routes for mobile ad-hoc networks. Proceedings of ACM MOBIHOC; 2003. p. p291–302.
21. Zhu B, Wan Z, Bao F, Deng R H, Kankanhalli M. Anonymous secure routing in mobile ad-hoc networks. IEEE Proceedings Conference on Local Computer Networks; 2004. p. 102–8.
22. Seys S, Preneel, ARM: Anonymous routing protocol for mobile ad hoc networks. IEEE International Proceedings Conference on Advanced Information Networking and Applications; 2006. p. 133–7.
23. Song L, Korba L, Yee G. AnonDSR: Efficient anonymous Dynamic source routing for mobile ad-hoc networks. Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks; 2005. p. 33–42.
24. Dong Y, Chim T W, Li VOK, Yiu S M, Hui CK. ARMR: Anonymous routing protocol with multiple routes for com¬munications in mobile ad hoc networks. Ad Hoc Networks. 2009; 7(8):1536–50.
25. Boukerche A, El-Khatib K, Xu L, Korba L. SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. Proceedings of EEEL CNpp; 2004. p. 618–24.
26. Amiri R, Rafsanjani MK, Khosravi E. Black hole attacks detection by invalid Ip addresses in Mobile Ad Hoc Networks. IJST. 2014 Apr; 7(4):401–8.