International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences
(NCDATES- 09th & 10th January 2015)

RESEARCH ARTICLE OPEN ACCESS

Detection And Prevention Of Misrouting And Colluding Collision Attacks In Wireless Adhoc Networks

K.Gurubrahmam[1] A.Hariprasad Reddy[2]
M.Tech Student, JNTUACE, PULIVENDULA 1
ASSISTANT PROFESSOR, DEPT.OF CSE, JNTUACEP PULLIVENDULA2

ABSTRACT
In several applications like Underground Mining, Military and navy, wireless Ad-hoc Networks play a significant role. because of this quality and benefits its wide used for several functions, however because of stealthy attacks there are heap of Packet drops because of Misrouting, Power management, identity delegation and colluding collusion .Wireless Ad-hoc Networks are particularly attractive and expensive to deploy vital networking infrastructure. To stop attacks in Wireless Ad-hoc Networks, current existing methodology is local watching. however these ways don't sight these forms of attacks in associate economical Manner and it ends up in malicious node drops information (entirely or selectively) passing through it or delays its forwarding and misrouting attack that during which within which} the aggressor relays packets to the incorrect next-hop which has the result that the packet is indirectly born. These attacks may lead to a big loss of knowledge or degradation of network practicality. In projected system we tend to return up with a brand new methodology known as SADEC that is capable of eliminating varied ways of packet dropping like Misrouting, and colluding collusion. SADEC Protocol collects information regarding native path and conjointly info concerning the neighbours. Except for native watching extra checking Schemes are enabled to watch the nodes endlessly to envision the Packet drops because of unwanted nodes. Therefore by effectively adding routing path info regarding the neighbours and conjointly taking the responsibility of checking for all the neighbours lurking attacks is all avoided from the ad-hoc networks.

Key words: Misrouting, colluding collision, local monitoring, packet dropping, SADEC

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- manage with none infrastructure. During this method, ad-hoc networks have a dynamic topology such nodes will simply be part of or leave the network at any time. they need several potential applications, especially, in military associate in attention rescue areas like connecting troopers on the field of battle or establishing a brand new network in suit of a network that folded once a disaster like an earthquake. Ad-hoc networks are appropriate for areas wherever it\'s insufferable to line up a set communications. Since the nodes communicate with each other one Associate in while not an infrastructure, they supply the property by forwarding packets over themselves.

Differing kinds of check square measure done domestically on the ascertain traffic to create a determination of malicious behavior. As an example, a node might ensure its neighbor is forwarding a packet to the right next-hop node, at intervals acceptable delay bounds. For systems wherever inward at a typical read is vital, the node initiates a distributed protocol to distribute the alarm. we tend to decision the present approaches that follow this guide Baseline local monitoring (BLM). Several protocols are engineered on prime of BLM for intrusion detection building trust and name among nodes protective against management and information traffic attacks and in building secure routing protocols. For specificity, we are going to use because the representative BLM that we are going to use for comparison with the approach conferred during this paper. In BLM, a bunch of nodes, referred to as guard nodes perform native observance with the target of sleuthing security attacks. The guard nodes square measure traditional nodes within the network and perform their basic practicality additionally to observance. Observance implies verification that the packets square measure being reliably forwarded while not modification of the immutable elements of the packet, at intervals acceptable delay bounds and to the suitable next hop. If the quantity of traffic is high (say for information traffic in an exceedingly loaded network), a guard node verifies solely a fraction of the packets.

In this paper, we tend to introduce a brand new category of attacks in wireless multi-hop accidental networks referred to as sneak packet

dropping. In sneak packet dropping, the offender achieves the target of disrupting the packet from reaching the destination by malicious behavior at associate degree intermediate node. However, the malicious node offers the impression to its neighbors taking part in native observance that it's performed the desired action (e.g., relaying the packet to the right next-hop on the way to the destination). This category of attacks is applicable to packets that square measure neither acknowledged end-to-end nor hop-by-hop .Due to the resource constraints of information measure and energy, a lot of traffic in multi-hop accidental wireless networks is unacknowledged or solely by selection acknowledged this can be significantly true for the a lot of common information traffic or broadcast management traffic than for rare uncast management traffic.

We provide a protocol called SADEC (**S**tealthy **A**ttacks in Wireless Ad Hoc Networks: **De**tection and **C**ountermeasure) that is built using local monitoring and that can mitigate each of the two attack types introduced above. The SADEC detection technique involves two high level steps: *first*, having guard nodes maintain additional next-hop information gathered during route establishment; and *second*, adding some checking responsibility to each neighbor. The latter technique makes use of the fact that under three of the attacks, neighbors have differing views of a node in terms of amount of forwarding traffic generated by the node. Hence, a single one-hop broadcast cannot convince *all* the neighbors. On the other hand, we show that of the two modes of the stealthy packet dropping attack, BLM is unable to detect any instance of two attack types. Any work that relies on BLM for building higher level knowledge (such as, reputation scores as in would suffer from the disadvantage of BLM against stealthy packet dropping.

.

II. LITERATURE SURVEY

Issa Khalil [1] we've introduced a replacement category of attacks known as sneak packet dropping that disrupts a packet from reaching the destination by malicious behavior at associate degree intermediate node. this could be achieved through misrouting, dominant transmission power, malicious electronic countermeasures at associate degree opportune time, or identity sharing among malicious nodes. However, the malicious behavior can't be detected by any behavior based mostly detection theme given thus far. Specifically, we tend to showed that basic native observation (BLM) based mostly notice ion cannot detect these attacks. in addition, it'll cause a legitimate node to be defendant. we tend to then given a protocol known as SADEC that with success mitigates all the given attack. SADEC builds on native observation and needs nodes to take care of further routing path info and adds some checking responsibility to every neighbor.

Yi-an Huang [2] during this paper, we've according our progress in developing intrusion detection techniques for Manet. Building on our previous work on native anomaly detection, we tend to any investigated the way to offer additional correct info on attack sorts once associate degree anomaly is found. Jay dip fractional monetary unit.[3]In this paper, we've projected a theme that allows routing protocols in MANETs to notice packet dropping by a malicious node. Every node within the network severally monitors the behavior of its neighbors. Issa Khalil [4] introduced a replacement category of attacks known as sneak packet dropping through packet misrouting that disrupts a packet from reaching the destination by malicious behavior at associate degree intermediate node. Angel female parent Alex [5] As wireless network threats have become additional dangerous day by day, security in wireless is most essential. Issa Khalil [11] we've introduced a replacement category of attacks known as sneak packet dropping that disrupts a packet from reaching the destination by malicious behavior at associate degree intermediate node. this could be achieved through one in every of four attacks types– misrouting, dominant transmission power, malicious jam at associate degree opportune time and malicious identity sharing.

III. Performance Metrics

In the evaluation transport protocols different performance metrics are used. They show different characteristics of the whole network performance. In this performance comparison evaluate the packet loss, throughput, End-to-End delay, packet delivery ratio of selected protocols in order to study the effects on the whole network. I report four performance metrics for the protocols:

- Packet loss: The number of data packets not received by the destination node to the number of data packets sent by the source node.
- End-to-end delay: This is the average time delay for data packets from the source node to the destination node. To find out the end-to-end delay the difference of packet sent and received time was store and then dividing the total time difference over the total number of packet received gave the average end-to-end delay for the received packets. The performance is better when packet end to-end delay is low
- Throughput: How much data can be transferred from one location to another location in given amount of time.
- Packet delivery ratio: The ratio of total no .of packets successfully received by the destination

nodes to the no. of packets sent by the source node.

IV. BACKGROUND: LOCAL MONITORING

In this section, BLM is delineate that is employed as a benchmark to judge the performance and effectiveness of SADEC in mitigating concealed packet dropping through misrouting and colluding collision attacks. Native watching by a node is outlined because the method of watching the traffic stepping into and out of its neighbors. This can be a cooperative detection strategy wherever the operate of watching is that the packets area unit verified whether or not they area unit being dependably forwarded with none modification to the suitable next hop. As shown in Figure.2, Imagine B is causing a packet to X that is to be relayed to D through A. when the packet is being forwarded to A, the guard nodes of A (X, M and N) that area unit within the transmission vary of A are going to be watching the intermediate node A to verify whether or not the packet is relayed to the Destination D or not. The nodes that area unit within the same transmission vary area unit same to be that nodes neighbors and that they act as guards for that node once a packet is to be forwarded by that node. It keeps the forwarding info in a very watch buffer with a timestamp. The packet must be send inside that point to the suitable next hop. In BLM, the doable suspicious behaviors of nodes will be known with the assistance of a bunch of nodes, known as guard nodes. MalC (G, R) refers to the MalC at the guard G that maintains all the suspicious actions of R over the packets send into R. If any malicious activity of R is detected by guard G, the MalC (G,R). is incremented. The increment to malc depends on the character of the malicious activity detected. Once the worth of MalC(G,R) crosses a threshold rate (MalCth) over Twin, node G revokes R from its neighbor list. During this case node G directly isolates node D. to boot G sends associate attested conscious of all the neighbors of R indicating that R could be a suspected malicious node. once a neighbor of R, say B, gets enough alert messages regarding R, node B revokes R. during this case B indirectly isolates R. This creates an area Isolation of a malicious node by its current neighbors

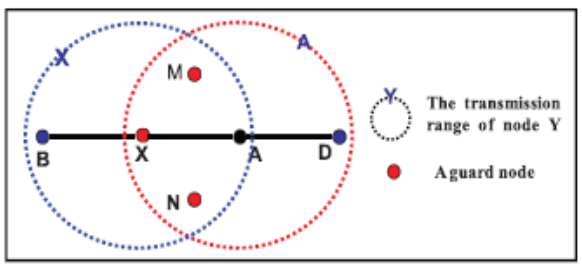

Fig 1: X, M, and N are guards of A over X->A

V. STEALTHY DROPPING ATTACK DESCRIPTION

In all the modes of concealed packet dropping, a malicious intermediate node achieves identical objective as if it were dropping a packet. However, none of the guard nodes exploitation BLM become any wiser attributable to the action. Additionally, a legitimate node is defendant of packet dropping. Next, we tend to describe the four attack varieties for concealed dropping

5.1 Drop through Misrouting:

In misrouting attack, a malicious node relays the info packets to wrong next hop, which ends up in packet drop. Note that, in Base line local monitoring a node that receives a packet to relay while not being within the route to the destination either drops the packet or sends a one-hop broadcast that it's no route to the destination. Consider the instance situation in Fig. 1. Node A sends a packet to the malicious node M to be relayed to node B. Node M simply relays the packet to node E that isn't within the route to the final destination of the packet. Node E drops the packet. The result's two fold: 1) node M with success drops the packet while not being detected since all the guards of M over A→M (regions I and II) are relieved by the transmission of M → E and 2) legitimate node E are going to be incorrectly defendant by its guards over M → E (regions II and III) as maliciously dropping the packet

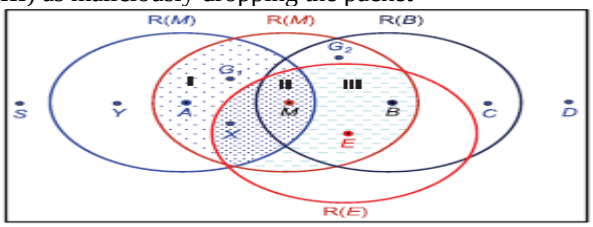

Fig 2: Misrouting situation

5.2Drop through Colluding Collision:

In several wireless sensing element network readying situations, the 802.11 mackintosh protocol RTS-CTS mechanism that reduces frame collisions owing to the hidden terminal drawback and therefore the exposed terminal drawback are disabled for the sake of energy saving. usually this can be} conjointly explained by the actual fact that packets in some wireless networks like sensing element networks are often quite little and fall below the brink for packet length that RTS/CTS is turned on. The wrongdoer might exploit the absence of the RTS/CTS frames to launch a sneak packet dropping attack through collision elicited by a colluding node.

The colluding node creates a collision within the neck of the woods of the expected next-hop node at associate degree opportune time. take into account the state of affairs shown in Figure four. The malicious node money supply receives a packet from S to be relayed to T. Node money supply coordinates its transmission with a transmission of some information generated by its colluding partner money supply to T. It has the impact that T is unable to induce the packet relayed by money supply. The injury caused by this attack is twofold: (i) money supply with success drops the packet owing to a collision at T while not being detected, and (ii) node T is defendant of dropping the packet by a number of its guards over the link M1->T (the guards that ar out of the vary of money supply, region I). Note that for money supply to be able to send information to T, it's needs to be a legitimate neighbor (compromised by the attacker), otherwise, the attack would be thought-about a physical layer electronic countermeasures , that is assumed to be detectable through techniques complementary to it given within the paper

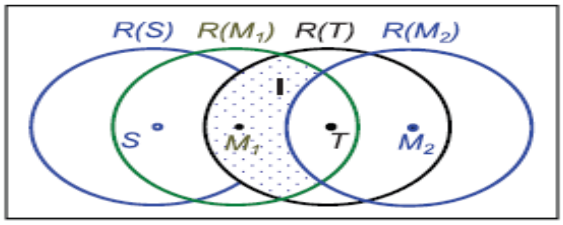

Fig3: Colluding Collision scenario

VI. STEALTHY DROPPING ATTACK MITIGATION

In SDAR, we propose two mechanisms to augment traditional local monitoring (LM) to enable the detection of stealthy packet dropping attacks. The first mechanism reduces (mitigates) stealthy packet dropping through misrouting while the second mitigates the rest of the attack types.

6.1 Mitigating misrouting attack

To observe this attack kind, native watching should incorporate extra practicality and data. the essential plan is to increase the information at every guard to incorporate the identity of subsequent hop for the packet being relayed. this extra information is collected throughout route institution. to gather the next-hop identity info in AODV, the forwarder of the REQ attaches the previous 2 hops to the REQ packet header. Let the previous hop of M be A for a route from supply S to destination D, and also the next hop from M be B (Fig. 3. once M broadcasts the REQ received from A, it includes the identity of A and its own identity (M) within the REQ header . once B and also the different neighbors of M get the REQ from M, they detain a Verification Table (VT) (last field is presently blank). once B broadcasts the REQ, the common neighbors of M and B update their VT to incorporate B. once B receives a REP to be relayed to M, it includes therein REP the identity of the node that M must relay the REP packet to, that could be a during this example.

Therefore, all the guards of M currently grasp that M not solely must forward the REP however conjointly that it ought to forward it to A. 2 tasks are intercalary to the practicality of the guards in watching the REP packets. First, the guard G of a node N verifies that N forwards the REP to the proper next hop. within the example on top of, G2 verifies that M forwards the REP to A. Second, G verifies that N has updated the forwarded REP header properly. Within the example shown on top of, G2 verifies that once the input packet to M from B is , then the output packet from M ought to be . Note that M and its guards over the link B →M grasp that subsequent hop could be a from the knowledge collected within the VT table throughout the REQ flooding. Exploitation the extra information mentioned on top of, SADEC detects misrouting attacks as follows: within the example on top of, assume that S is causation a knowledge packet to D through a route that features .

The malicious node M cannot misroute the information packet received from A to a node apart from subsequent hop, B since every guard of M over the link A→M has associate degree entry in its VT that indicates B because the correct next hop. This leads to an extra checking activity for the guard node concerned in native monitoring—verifying that the information packet is forwarded to the proper next hop, as indicated by the entry within the guard node's VT.Moreover, M cannot frame another neighbor, say X, by misrouting the packet to X. The guards of X over M → X don't have associate degree entry like and thus, they'd not increment the MalC of X once it drops the packet.

6.2 Mitigating Colluding Collision Attack

The attacker defeats the native watching primarily based detection by reducing the amount of guards that catch a packet to zero or to variety but the arrogance index. The colluding collision attack, the assaulter evades detection by satisfying all the nodes. The planned measure needs increasing the set of nodes that may guard a node thus on embrace all the neighbors of the node being monitored. beneath the stealthy packet dropping attacks, the neighbors have totally different views of a node in terms of the amount of packets it's forwarded and thus all the neighbors can't be convinced if that node is malicious.

The SADEC technique makes use of this reality. to attain this goal, extra tasks got to lean to the nodes within the network. A preset quantity is nominal node ought to keep a count of the amount of messages each of its neighbors had forwarded. every node should announce the amount of packets it's forwarded over some amount of your time.

By forcing a node to announce the amount of messages it's forwarded over some amount of your time, a malicious node would got to face the matter of satisfying all the neighbors World Health Organization expects constant count. A neighbor of the node that collects the amount of forwarded by that node and comparison the result with the count that has been proclaimed by the node is named comparator. If the comparator's count isn't inside the suitable vary of the proclaimed forward count, it increments its malicious counter for the saying node

VII. SIMULATION RESULTS

Performance analysis of Stealthy attacks in misrouting

Table 2:Time vs. Delivery ratio, End to end delay, throughput and Packets dropped for misrouting attack

Time	Packet delivery ratio	End -to-end delay	Throughput	Packets dropped
10	0.4244	29.3749	447.61	198
20	0.4646	29.81	480.57	408
30	0.4779	29.609	491.41	615
40	0.4831	29.3206	496.58	825
50	0.4871	29.4035	499.89	1032

Performance analysis of SADEC scheme

Delivery ratio, End to end delay, throughput, Packets dropped are measured for SADEC (Stealthy Attacks Detection and Countermeasure) scheme and outputs are shown using graphs.

Table 3: Time vs Delivery ratio, End to end delay, throughput, Packets dropped are measured for SADEC.

Time	Packet delivery ratio	End –to-end delay	Throughput	Packets dropped
10	0.9470	18.9304	604.86	25
20	0.9282	28.4149	620.77	75
30	0.9195	32.0651	623.54	130
40	0.9369	16.7115	636.52	138
50	0.9503	4.3957	646.49	137

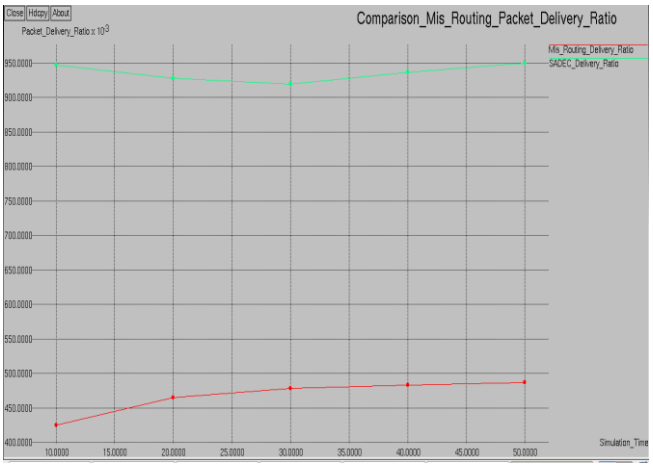

Fig 4: Comparison of Misrouting packet_delivery_Ratio, SADEC delivery ratio,

Source node send RREQ send to all nodes .The misrouting attacker node send first reply to the source node .Source node accept the first reply from attacker node, and misroute the packets from source to attacker.

Attacker node didn't send any packets to destination, and there is no packet transmission to destination.

But in sadec prevention system source node successfully transmit the packets to destination.so; comparison of sadec is good performance in packet delivery ratio.

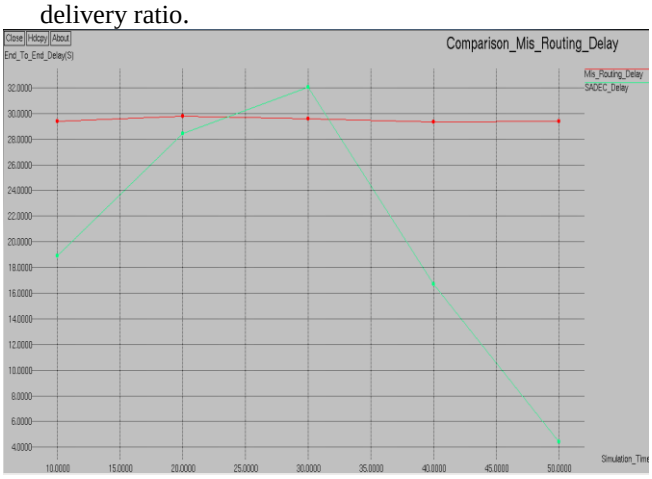

Fig 5:Comparison of Misrouting delay, SADEC delay,

This is a reactive routing protocol.suppose link failure occurs means path will be changed.

Path will be changed means some delay will occur. In before misrouting attack there is no path change. Here every time path will be updating.so,delay will be more.

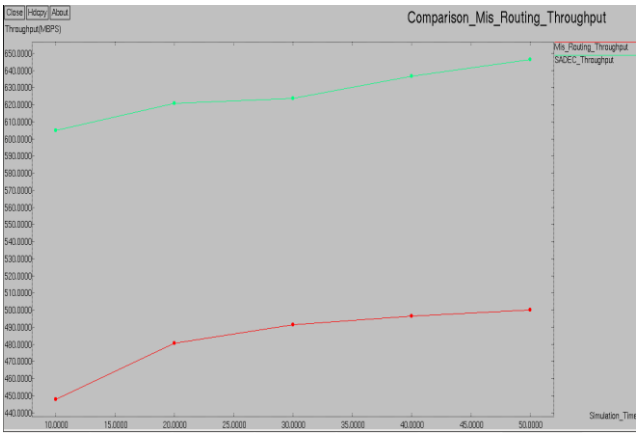

Fig 6:Comparison of Misrouting throughput, SADEC throughput

Successfully transmission of packets from source to destination is less, because of misrouting attack.

After prevention of sadec successfully transmitted the packets from source to destination then the throughput will increase.

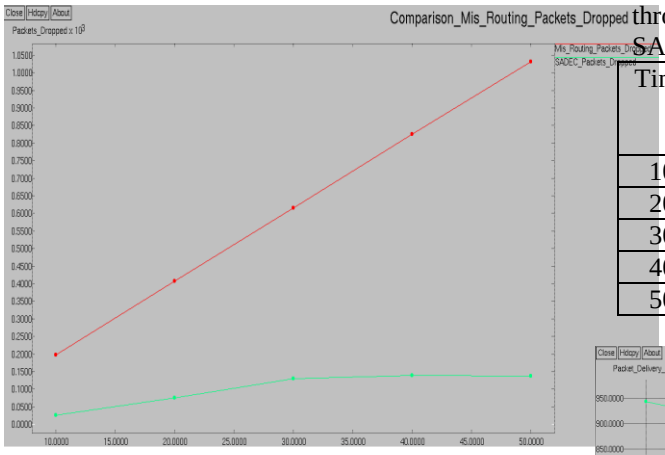

Fig7: Comparison of Misrouting_packets_dropped, SADEC packets dropped

The transmission of packets from source to destination packets dropped is more because of misrouting attack.

But in sadec prevention system packets dropped are less compared to misrouting attack

Performance analysis of Stealthy attacks In colluding collision attack

Table 2.Time vs. Delivery ratio, End to end delay, throughput, Packets dropped for colluding collision attack

Time	Packet delivery ratio	End –to-End delay	Throughput	Packets dropped
10	0.3635	23.0326	492.54	345
20	0.3464	21.4825	502.50	764
30	0.3424	21.1423	505.91	1179
40	0.3397	20.8975	507.40	1598
50	0.3384	20.8939	508.43	2014

Performance analysis of SADEC scheme in colluding collision attack

Delivery ratio, End to end delay, throughput, Packets dropped are measured for SADEC (Stealthy Attacks Detection and Countermeasure) scheme and outputs are shown using graphs.

Table 1.3: Time vs. Delivery ratios, End to end delay, throughput, Packets dropped are measured for SADEC.

Time	Packet delivery ratio	End – to-end delay	Throughput	Packets dropped
10	0.9089	72.4899	594.19	43
20	0.8966	49.9373	607.86	108
30	0.9232	31.2079	626.96	124
40	0.9433	17.3729	641.89	124
50	0.9554	9.64798	650.79	123

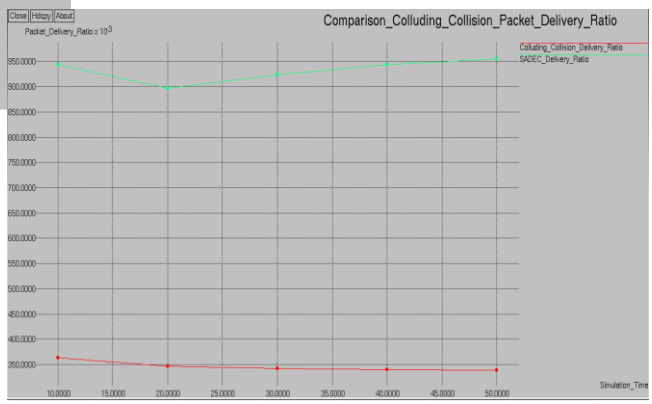

Fig8:Comparison_of colluding_collision packet_delivery_Ratio, SADEC delivery ratio

The transmission of packets from source to destination is not received because of colluding collision attack.so,packet delivery ratio is less.

In sadec packet delivery ratio is more and the transmission of packets from source to destination

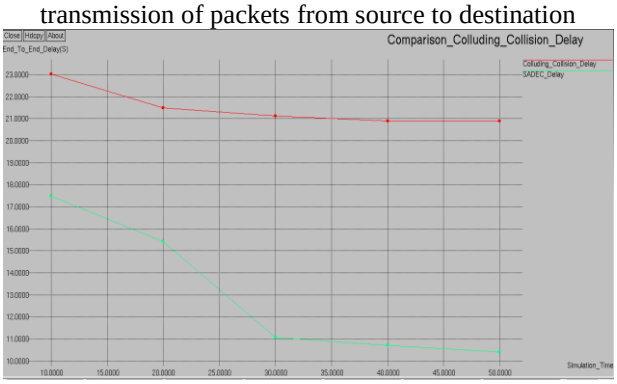

Fig 9:Comparison of colluding collision delay, SADEC delay,

In colluding collision attack there are average no. of hops between source to destination.

But in sadec system no. of hops will be more in source to destination. So, end to end delay is slightly increased than colluding collision attack.

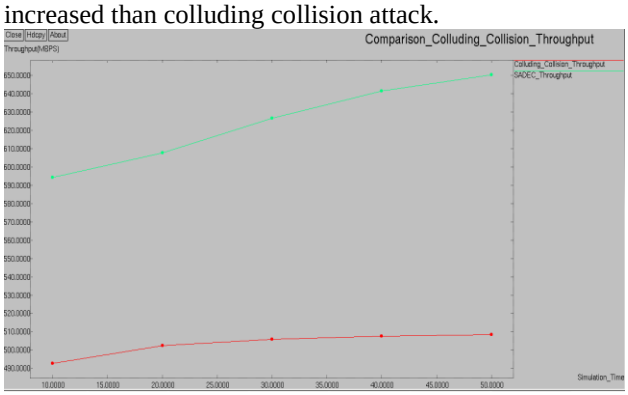

Fig 10:Comparison of colluding collision throughput, SADEC throughput

Successfully transmission of packets from source to destination is less, because of colluding collision attack. After prevention of sadec successfully transmitted the packets from source to destination then the throughput will increase

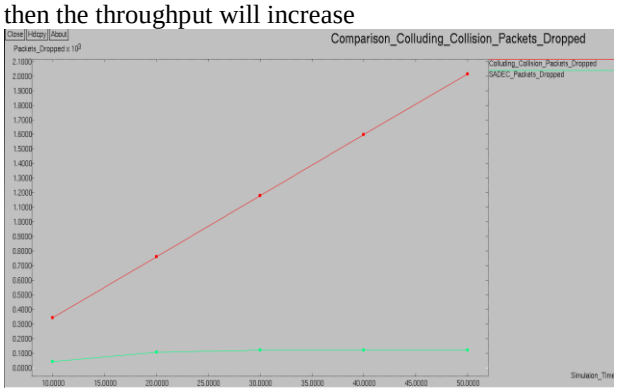

Fig 11:Comparison of colluding collision Packets dropped, SADEC Packets dropped

The malicious nodes are not transmitting to any other nodes.so; consider these packets are dropped packets. But in sadec all the nodes are forwarding packets. So, less packets are dropped compared to colluding collision attack.

VII. CONCLUSION:

We have introduced a new class of attack which disrupt a packet from reaching the destination by malicious behavior at an intermediate node. This can be achieved through misrouting and colluding collision. However, the malicious behavior cannot be detected by any behavior based detection scheme presented to date. Specifically, we showed that BLM-based detection cannot detect this attack. We then presented a protocol called SADEC that successfully mitigates all the presented attack. SADEC builds on local monitor and requires nodes to maintain added routing path information and adds some checking responsibility to each neighbor. Additionally, SADEC's new detection approach expands the set of neighbors that are capable of monitoring in a region, thereby making it more suitable than BLM in sparse networks.

In future work, we are considering other detection techniques for multiradio wireless networks such as power control, and identity delegation. The listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels and multiple radio networks

References:

[1] Issa Khalil and Saurabh Bagchi: Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure Digital Object Indentifier 10.1109/TMC.2010.249

[2] Y. Huang and W. Lee, :"A Cooperative Intrusion Detection System for AdHoc Networks," in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pp. 135-147, 2003.

[3] aydip Sen Piyali Roy Chowdhury, Indranil Sengupta: "A Distributed Trust Mechanism for Mobile Ad Hoc Networks" 1-4244-0731-1/06/$20.OO ©2006 IEEE.

[4] Issa Khalil MIMI: Mitigating Packet Misrouting in Locally Monitored Multi-hop Wireless Ad Hoc Networks 978-1-4244-2324-8/08/$25.00 © 2008 IEEE.

[5] Angel Mary Alex, M. Ashwin: Detection of Colluding Collision and Identity Delegation Attacks in Wireless Ad Hoc Networks via SADEC 2013 IJARCET

[6] Praveen Kumar Karri, Jashwanth Kumar Avujuri: SADEC PROTOCOL FOR DETECTING AND PREVENTING STEALTHY ATTACKS IN WIRELESS ADHOC NETWORKS 2012 IJAIR
[7] E.S.Phalguna Krishna* , I.D.Krishna Chandra: Packet Misrouting Attacks in Multi Radio Wireless Networks: Detection and Countermeasure
[8] Yafeng Wu, John A. Stankovic, Tian He† , and Shan Lin: Realistic and Efficient Multi-Channel Communications in Wireless Sensor Networks
[9] Asad Amir Pirzada and Chris McDonald: Establishing Trust In Pure Ad-hoc Networks The University of Western Australia 35 Stirling Highway, Crawley, W.A. 6009, Australia.
[10] Richard Draves Jitendra Padhye Brian Zill]: Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks Copyright 2004 ACM 1-58113-868-7/04/0009 ...$5.00.
[11] Issa Khalil, Saurabh Bagchi," MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-hop Wireless Ad Hoc Networks", Conference name: Secure Comm 2008, September 22 - 25, 2008