ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Detection of Colluding Collision and Identity Delegation Attacks in Wireless Ad Hoc Networks via SADEC

Angel Mary Alex, M. Ashwin

***Abstract*— The colluding collision and identity delegation attack comes under the new class of attacks of wireless ad hoc networks namely stealthy attacks that diminish the expense and sight of the invader. The nodes which are compromised by these attacks provide the impression to their neighbors as if they are doing the correct forwarding action. The normal nodes will be accused of showing malicious behavior. In the colluding collision attack, the adversary injects malicious nodes at the opportune time so that collision will occur and hence, the packet will not reach the destination. In case of identity delegation attack, the malicious nodes relay their identities to some other compromised node in the network so as to make the packet which it receives to be delivered to a wrong next hop by making use of that delegated identity. Observation of the behavior of the neighborhood which is performed by the normal network nodes is one of the common methods for detecting attacks in wireless networks. Local monitoring also does the same but these cannot detect stealthy attacks efficiently as they isolate legitimate nodes mistakenly. This drawback can be rectified using a protocol called SADEC. It makes use of the local monitoring technique by increasing the number of nodes that can do the monitoring function and they maintain additional information about the routing path so that it can check whether each node is doing its legitimate action.**

***Index Terms*—Ad Hoc networks, local monitoring, Stealthy packet dropping, Colluding collision, Identity delegation**

I. INTRODUCTION

An ad-hoc network is a collection of wireless mobile nodes that forms a temporary network without the help of any centralized administration. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, hence it is well suited for the scenarios in which pre deployed infrastructure support is not available. Each mobile node operates not only as a host but also as a router that forwards the packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad-hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. The mobility of the routers are provided randomly and organized themselves arbitrarily; thus, the network's wireless topology may alter rapidly and unpredictably.

Manuscript received Feb , 2013.

***Angel Mary Alex**, Department of CSE, Adhiyamaan College of Engineering Hosur,T.N,India*

***M.Ashwin**, Department of CSE, Adhiyamaan College of Engineering Hosur,T.N,India.*

II. THREATS IN AD HOC NETWORKS

The security issue of an ad hoc network is of great concern while considering its various factors like its open network, mobility factor and other factors. The attacks on an ad hoc network can be classified into two; internal attacks and external attacks. Internal attacks are those attacks which are caused by an inside node of a network. These attacks are produced by either malicious nodes or by selfish nodes inside a network. These internal attacks are difficult to detect as the nodes affected by such an attack generate themselves the valid signatures using their private keys[8].Examples of internal attack are internal eavesdropping, where the nodes extracts copy of all information and exploited it without the knowledge of other nodes and packet dropping.

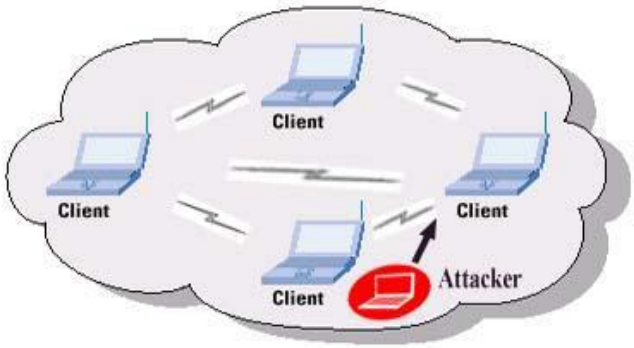

Fig 1: Internal attack

In external attacks, the attackers are from outside the network but causes damage or compromises network within the network. Attacks from external nodes can be prevented from cryptographic techniques such as encryption and authentication. As per routing, external attacks can be divided into active and passive attacks. Active external attacks degrades or stops message flow between the nodes.Some examples of active external attacks are DoS attacks, packet dropping stealthy attacks or flooding of packets. Passive external attacks are formally done by compromising the nodes and extracting vital information of the network. In passive attack, the attacker does not disrupt the network operation but only extracts information to damage further network

operation. These type of attacks are basically impossible to detect, thus making it hard to produce security for such attacks.

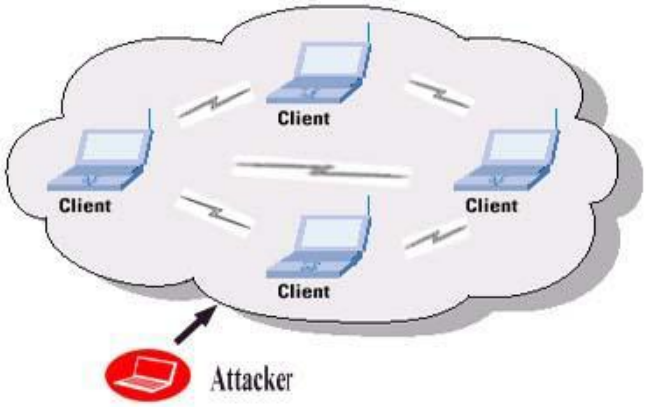

Fig 2: External attack

In wireless ad hoc networks stealthy attacks are a new class of attacks which are performed silently and cautiously, so that nobody notices what the attacker is doing. It consists of four attacks- misrouting, power control, colluding collision and identity delegation. The objective of the attacker is not only to successfully implement the attack, but also to do so with a less energy and effort, and in a way that hides their existence and whereabouts to the largest possible extent. From the attacker's point of view, a stealthy attack is better than an attack that requires a larger amount of his energy and which leaves him more exposed to detection. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. The malicious node gives the impression to its neighbors that it performs the legitimate forwarding action. A legitimate node comes under suspicion. These attacks can be easily breakdown the multi-hop wireless ad-hoc networks.

III. SECURITY CHALLENGES IN MANET

The nature of MANET makes it vulnerable to attacks. Challenges in MANET securities are discussed briefly:

Availability: should withstand survivability regardless of Denial-of-Service (DOS) attacks like in physical and media access control layer attacker uses jamming techniques for hinder with communication on physical channel. On network layer the attacker can interrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

Confidentiality: should protect certain information which is not to be disclosed to unauthorized entities.

Integrity: Transmitted message should be genuine and should never be modified or corrupted.

Authentication: Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes.

Non-repudiation guarantees that the source of a data should not reject having sent the data.

IV PROBLEM IDENTIFICATION & PROPOSED SOLUTION

Colluding collision attack disrupts a packet from reaching its destination by malicious collusion at intermediate nodes. In this mode, the attacker uses a colluding node (external or internal) in the range of D to transmit data at the same time when M starts relaying the packet to D. Therefore, a collision occurs at D, which prevents the packet from being correctly received by D, while M appears to be performing its functionality correctly.

In the identity delegation attack mode, the attacker colludes with a node E placed close to the source node S. E is allowed to use M's identity and transmit the packet. Since E is almost at the same place as S, D does not receive the packet while the guards of M are deceived that M relays the packet to the next hop. In each of these attack types, the adversary can successfully perform the attack without detection. Additionally, in each attack type, a legitimate node is accused of packet dropping.

A protocol called SADEC is introduced that can detect and isolate stealthy packet dropping attack efficiently. SADEC presents two techniques takes two steps. First, it extends the number of guards from only the common neighbors of the relaying node and the next hop to include all the neighbors of the relaying node. Second, it creates a counter at each node for each neighbor which is responsible for counting the number of forwards by that neighbor. The latter technique makes use of the fact that under the colluding collision attack, the attacker tries to divide the neighbors into two sets having differing views in terms of the amount of forwarding traffic generated by the attacker. SADEC improves the efficiency of the wireless ad-hoc network over the base line local monitoring.

V.STEALTHY ATTACK MODEL AND SYSTEM ASSUMPTIONS

Attack Model

In this attack, the adversary is powerful because it has the resources to gain control over the legitimate nodes. The basic aim of this attacker is to capture all the information from a particular node and copy this to another node, making that node look like a legitimate node belonging to this network. In the process it tries to eliminate the original node from the network, to ensure that two copies of the same node aren't discovered. The newly formed malicious nodes have more power than their original counterparts and will be able to vary their transmission ranges and communicate via different channels.

System Assumptions

A few assumptions are required for this attack to be successfully implemented. The nodes use the three handshake methods to begin their communication. The two malicious nodes are designated as M1 and M2. These nodes have to be placed in the particular places for the attack to be successful. As shown in figure 3 the Euclidian distance between the malicious node (M1) and the attacked node (C) should be less than or equal to the malicious node's transmission range (R1), which is given in Equation (1).

$$d(M1,C) < R1 \quad (1)$$

The adversary has to make sure that the transmission range of the second malicious node (M2) is less than the normal

transmission range (R1). The normal transmission range (R1) should be less than the transmission range of the synchronizing messages (RSync). This is given in Equation (2).

$$R2 < R1 < RSync \quad (2)$$

To make sure that the malicious nodes can send at the same time and will not interfere with each other, the adversary must satisfy Equation (3). Where the second malicious node (M2) should be out of the first malicious node (M1)'s range.

$$d(M1,M2) >= R1 \quad (3)$$

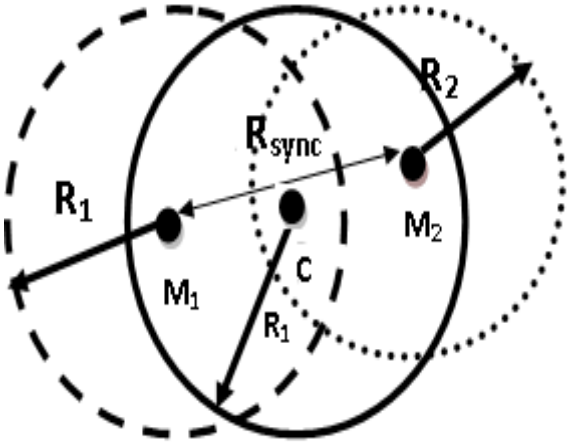

Fig 3: Injected Malicious Nodes Placement

Colluding Collision Attack in MANETs

Malicious nodes M1 and M2 are injected into the network by the adversary. These nodes then decide to attack a particular node, say the destination. This causes packets to be dropped , thus passing the blame to the destination for being malicious. This node then has to be removed from the network to prevent further packet loss.

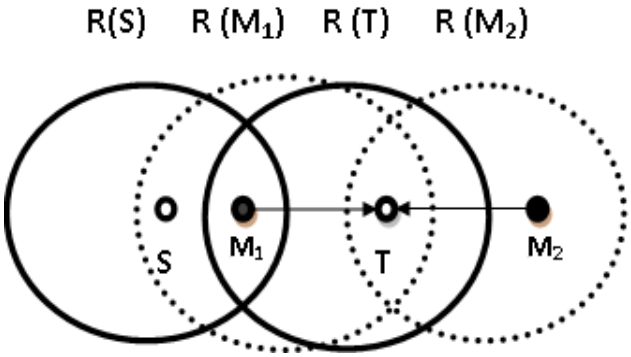

Fig 4: Attack scenario for Colluding Injected Attack.

Consider the scenario shown in the figure 4, where the source S is trying to send packets to T but these have to be sent through M1. At the same time M1 sends its packets to T, M2 will also send packets to T. This simultaneous transmission creates a collision at T which prevents it from correctly receiving the packet relayed by M1.

The malicious nodes will attack one node after the other thereby the attack spreads to the entire network. The damage caused by this attack is threefold: (i) the packets are dropped at T because of the collision, (ii) M1 is not suspected as the cause of the attack, and (iii) node T is falsely accused of dropping packets and isolated from the network.

Identity Delegation

In this form of attack, two malicious nodes are used by the attacker to drop the packet. One node is spatially close to the sender. The other node is the next hop from the sender[2].

Consider the scenario shown in Fig.5.The node s sends a packet to the malicious node M2 to be relayed to node T. The attacker delegates the identity and credentials of the compromised node M2 to a colluding node M1 close to the sender S. After s sends the packet to node M2, M1 uses the delegated identity of M2 and transmits the packet. The intended next hop T will not get the packet since it is not in the range of M1.The consequences of this attack are that the packet was successfully dropped without detection and the guards will accuse T for dropping the packet.

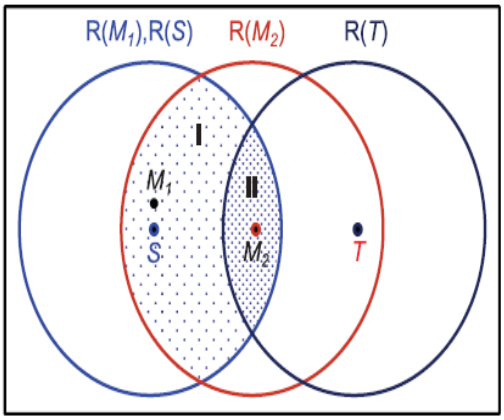

Fig.5. Identity Delegation illustration scenario

Guard Concept

When a node forwards a packet, the node's guards verifies that the next node in the path also forwards the packet. The guard does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving. In other words, every packet that is overheard by the guard is compared with the packet in the buffer to see if there is a match. A match confirms that the packet has been successfully delivered and it is removed from the buffer. If a packet has remained in the buffer beyond the timeout period then a failure counter for the node responsible for forwarding the packet is incremented. If this counter exceeds a predetermined threshold then the node is termed as malicious and the network is informed accordingly.

Proposed Algorithm

The proposed algorithm is to detect and eliminate the Colluding Collision and Identity Delegation Attack in Mobile Ad hoc Networks. This algorithm uses the concept of guard location monitoring[2] in order to detect malicious behavior in a network and this algorithm is implemented using the AODV protocol.

Algorithm

Step 1 In this algorithm, the number of guard nodes is extended from only the common neighbors of the relaying

node and the next hop to all the neighbors of the relaying node.
Step 2 Each node X, creates a counter (Fcount(x,y)) for each neighbor Y, which is responsible for counting the number of forwards by that neighbor over a time interval.
Step 3 These nodes try to divide the neighbors into two sets having differing views in terms of the forwarding traffic generated by the attacker.
Step 4 The guards broadcast a probe request packet (AODV_PROBE_BR) to all the nodes in its transmission range asking for the number of packets that particular node has transmitted.
Step 5 Each node replies with a probe reply packet (AODV_PROBE_REP) to the guard, which carries the count of the packets it has forwarded and its node identity (ID).
Step 6 The guard node creates a table with the information received from the probe packets from other nodes.
Step 7 The guard node then compares its table with the tables of other guard nodes.
Step 8 There is malicious activity due to the collusion attack and packets are dropped. A discrepancy arises when the tables are compared. This discrepancy is used to detect the malicious node and the attacker node.

Stealthy Attacks Scenario (with guards)

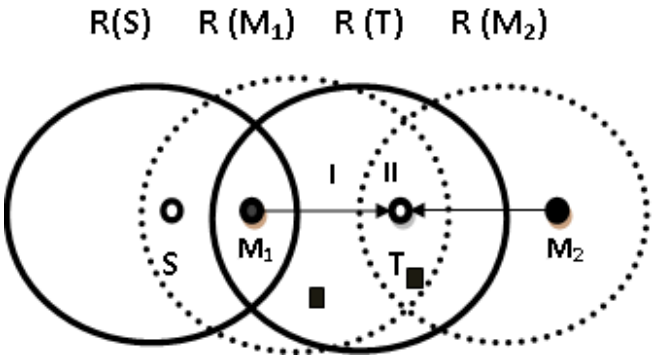

Fig 6: Attack Scenario with the guard nodes and malicious nodes

Where S is the source node, A and B are the guard nodes, M1 and M2 the malicious nodes and T is the destination node.

Route Establishment

The on-demand routing protocol, AODV (Ad Hoc On-demand Distance Vector routing Protocol) is used for route establishment. AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of route discovery and route maintenance from DSR and in addition it also uses the hop-by-hop routing, sequence numbers and periodic beacons from DSDV. Since AODV is a reactive protocol, whenever a node is ready for a data transmission (say source node S) to any other node (say destination D) it starts the route discovery process which is done by broadcasting a Route Request Packet (RREQ) to all its neighboring nodes. These packets are further transmitted to its neighbors and so on, until it finds a node which has a fresh route to the destination node (D) or the destination node itself. In either case the node replies with a Route Response (RREP) to the node from which it received the RREQ. This reply is transmitted in the reverse direction till it reaches the source node(S). The routing tables are updated by the intermediate nodes whenever they receive an RREQ or RREP packet with the next hop information.

Once the source node(S) reaches the RREP packet, it starts routing the data packets to the node from which it received the first RREP because it is usually the shortest path. The packet is further forwarded according to the next hop information of the intermediate nodes till it reaches the final destination.

Malicious Node Detection

The proposed algorithm first detects those nodes, which may be malicious. Then the neighbor of the malicious node initiates a cooperative detection mechanism to detect the actual black hole node. In AODV routing, messages contain only the source and the destination addresses. It uses destination sequence numbers to specify the valid route. At first the sender broadcast the Route Request (RREQ) message to its neighbors. Each node that receives the broadcast, checks the destination to see if it is the intended recipient. If yes it sends a Route Reply (RREP) message back to the originator. RREP message contains the current sequence number of the destination node. The same process continues till the packets reach to destination or reach to an intermediate node, which has a fresh, enough routes to destination. Every node keeps track of its neighbor by maintaining two small size tables. One is sequence table (SnT) to keep the neighbor node's id and neighbor node's sequence number and other is the status table (ST) to keep track of the node's status whether it is a safe node or a malicious one. Every node also maintains a neighbor list (N_List) and this list is updated periodically. When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value? if so then the intermediate node stops forwarding the message and mark the node as „M" or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious node's id and neighbor list of the malicious node. The threshold value is the average difference of Dst_Seq in each time slot between the sequence number of RREP message and the one held in the table.

VI. Simulation

The ns-2 simulation environment [3] is used to simulate a data exchange protocol, individually with BLM and with SADEC.The nodes are distributed randomly over a square field (1,500 m X 1,500 m) with a fixed average node density.

A generic on-demand shortest path routing protocol, say AODV, is used that floods route requests and unicasts route replies in the reverse direction. A route, once established, is not used forever but is evicted from the cache after an idle period TOutRoute if no other packet has been forwarded to the particular destination. A malicious node does not generate any data of its own. The simulation also accounts for losses due to natural collisions. The guards inform all the neighbors of the detected malicious node through multiple unicasts. For each simulation run, malicious nodes are chosen at random.

VIII Conclusion

As wireless network threats are becoming more dangerous day by day, security in wireless is most essential. A new class of attacks called stealthy packet dropping is introduced which disrupts a packet from reaching the destination by malicious behavior at an intermediate node. Stealthy Attacks are routing attacks allow a skilled but not very powerful attacker to target communication networks in a way that makes it unlikely that he gets traced and caught. This can be achieved through misrouting, controlling transmission power, malicious jamming at an opportune time, or identity sharing among malicious nodes. But, the malicious behavior cannot be detected by any behavior based detection scheme presented to date.

A protocol called SADEC (Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure) is presented that successfully mitigates all the presented attacks. SADEC is built on local monitoring which is a collaborative detection strategy where a node monitors the traffic going in and out of its neighbors and requires nodes to maintain additional 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 neighborhood, thereby making it more suitable than BLM in sparse networks.

The design of SADEC fundamentally relies on the ability of some guard nodes to overhear the behavior of neighboring nodes. Any technique that relies on this has the drawback that it can be bypassed by a powerful adversary that can accurately place malicious nodes capable of colluding with compromised nodes to create collision or delegates its identity to some other compromised node. But it is less susceptible to this drawback than prior techniques since it increases the number of nodes that are performing verification.

.

ACKNOWLEDGMENT

Our thanks to the experts who have contributed a lot towards the development of the stealthy attack and its simulated solution. We would like to thank GOD, the Almighty and everyone, just everyone!

REFERENCES

[1] A.A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-Hoc Networks," Proc. Australasian Conf. Computer Science (ACSC '04), vol. 26, no. 1, pp. 47-54,2004.

[2] Issa Khalil and S. Bagchi, "Stealthy Attacks in wireless Ad hoc Networks:Detection and Countermeasure",IEEE Transactions on Mobile Computing, vol.10,no. 8,August 2011.

[3] Issa M. Khalil, Abdallah Khreishah , " Dependable relief wireless sensor networks for reliable and secure humanitarian applications" , ELSEVIER journal on Ad Hoc Networks,2012.

[4] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2011

[5] I. Khalil, S. Bagchi, C. Nina-Rotaru, and N. Shroff, "UNMASK: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks,"Ad Hoc Networks, vol. 8, no. 2, pp. 148- 164, 2010.

[6] Farah Kandah, Yashaswi Singh, Chonggang Wang , Department of Computer Science, North Dakota State University, Fargo," Colluding Injected Attack in Mobile Ad-hoc Networks " in IEEE INFOCOM 2011 Workshop on M2MCN-2011

[7] I. Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. ACM Int'l Conf Security and Privacy in Commn. Networks(SecureComm'08),

[8] Rajaram Ayyasamy,"An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks," The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012

Angel Mary Alex received the B.Tech degree in Information Technology from the Mahatma Gandhi University, Kottayam, Kerala in 2010 and currently doing post graduation in Computer Science Engineering in Adhiyamaan College of Engineering, Affiliated to Anna University, Chennai. She can be reached at angelmaryalexk@gmail.com

M.Ashwin received the B.E. degree in Computer Science Engineering from the Periyaar University, Salem, TamilNadu, in 2004, the M.E. degree in Computer Science Engineering from the Anna University, Chennai, Tamil Nadu, in 2007, respectively. Currently, he is an associate Professor of Computer Science Engineering at Anna University.