# Identification of Misrouting in Wireless Adhoc Network

*Jayaprakash. N, *Sam Balaji. B, *Manikandan. J, **V. M. Gayathri
* Post Graduate Students
** Assistant Professor
Department of Computer Science and Engineering
Saveetha School of Engineering, Saveetha University, Chennai

*Abstract* - **Packet Misrouting or Packet losing is a collection of attacks such as misrouting, power control, identity delegation, and colluding packets that can be easily deployed against wireless ad hoc networks. This attack makes the loss of packets that need to be reached to destined node by an intermediate compromised node However, the compromised node performs forwarding packets, this makes impression of legitimate node to its neighbour's. In turn this makes a legitimate node as malicious node as it losses packets. A popular Behaviour based detection technique, Local monitoring helps in detecting this type of attacks.**

**This technique suffers in detection of appropriate compromised node which does malicious action and also it falsely removes a legitimate node from the network. Reactive routing protocol is used to finds path to destination on an on-demand basis requirement. Specifically, AODV (Adhoc On-Demand Distance Vector) routing protocol is used in this paper to avoid intrusion before transmitting packets. And also an additional functionality has been added to the AODV protocol to keep the next node value which in turn can be used to check the integrity of the node. Network simulator (NS-2) is been used to deploy this transmission.**

***Keywords— Misrouting, Adhoc Networks, AODV Routing Protocol, Baseline Monitoring***

## I. OVERVIEW OF WIRELESS AD-HOC NETWORK

Wireless ad-hoc networks are the networks that do not have any fixed infrastructure. Ad-hoc networks are termed as MANET (Mobile Ad-hoc Network) as the nodes in the network are always mobile (Nodes mobility flexible). A MANET network is a peer to peer network that can establish connection with every other node in the network when adequate radio signal is perceived from that node. If the defined node is not in range, it can able to en route its establishment through intermediate nodes, until it reaches the destined node.

### *A. Routing Basics:*

Routing is the process of finding path and moving packets across the internetwork from source to sink. At least one intermediate node is participated in the routing process.

### *B. Routing Components:*

Routing comprises of two activities: Determining routing path information and transferring packets through an internetwork commonly known as switching. As switching is performed by intermediate nodes, determining route is very difficult.

### *C. Path Determination:*

Path determination is the process of finding optimal path from source to destination along with appropriate routing protocol to transfer data in effective manner. To determine path length or routing path, routing algorithm is used. In every node a routing table is maintained which contain the routing information (Nearest neighbor) of the network is stored. Route information in the table differs over different routing algorithm used. Because routing algorithm is used to store the information about the network in its own way that is viable for transmission. Destined path is stored in the routing table of the nodes in the transmitting network that contains information of next hop/node until destination. When routers receive data, it checks for destination IP address and forwards packets to the nearest neighbour or shortest path to reach the destination address. Routers compare metrics to choose the optimal path that differs upon routing algorithms used. The routing update message is one such message that generally consists of all or a portion of a routing table that is broadcasted over the network so as to update the routing table of every other node in the network.

### *D. Routing Algorithms:*

Routing algorithm determines the routing path based on several different properties. Each routing algorithm has different impact on choosing the path to destination as well as storage of route information depending on the network infrastructure and the resources. Routing algorithm is deduced depending upon different performance metrics that is employed against network to get optimized route discovery. In this paper, Ad-hoc routing algorithm is used to determine the malicious node in the network with added special characteristics. Ad-hoc routing algorithm is a standard or protocol that determines the route to transmit packets between the source and sink in a wireless/mobile network. The topology of the Ad-hoc network isn't like other network, because the topology is determined at the time of discovery of route. Hence this routing algorithm is used to find the live nodes in the network (with in radio propagation area) at the time of transmission.

The Ad-hoc Routing Protocols are

- Proactive (Table-Driven) Routing
- Reactive (on-demand) Routing

Reactive routing protocol is used to find path on-demand basis which is very much useful in the wireless ad-hoc network.

- Source-initiated route discovery.
- Reduction in routing overhead.

No routing structure created a priori. Routing is only done when needed. Source floods the network through every other node in the network, a route request packet is broadcasted to obtain the information to destination. Flood is propagated outwards from the source. Pure flooding means every node transmits the request only once. Destination replies to request. Reply uses reversed path of route request sets up the forward path.

### E. *Network Simulator-2 Basics:*

NS2 is an open-source simulator and used for simulation of routing, multicasting, and for implementing protocols such as UDP, TCP, RTP and SRM over wired and wireless (local and satellite) networks. It is used for depicting graphically detailing of entire network traffic. And using this simulator, the programming can be done using Tool command language (TCL) and the results are displayed using the XGraph and Network Animator (NAM).

## II. AODV ROUTING PROTOCOL

Ad-hoc on demand distance vector routing protocol is used to find the route to destination on on-demand basis. As the mobile nodes in the network changes its course time to time, predefined route never had been a solution in the ad-hoc infrastructure. Aodv protocol floods the request to all over the network so that the destined network is pinged through the intermediate nodes. The next hop/node address is stored in the routing table of every node in the path retained by the AODV protocol. If the mobile node is out of range, the AODV protocol will find path from the link damaged and reroute the packets in an alternate path.

Counting to infinity problem is avoided in AODV protocol which offers quick convergence when the network is re-structured. When the node in the network is damaged, it is broadcasted to every other neighbour nodes of damaged node and it can prevent the data to be sent to an unreached node. AODV protocol's Destination Sequence Number is encoded with reply message from the destination to the source node. Through this, source can choose the path with the help of the destination sequence number.

### A. *Overview- AODV Routing*

Route request is made by the source systems to every node that is connected to the network and should be in radio range and Time to live (TTL) value is used to ensure the packet reaches the destination. If packet fails to reach, no response actions are recorded. Once the broadcasted request reaches the destined node, a route reply message is originated form the destination with the destination sequence number. The route reply message is transmitted back to the source address and the path is determined by the source systems. The packets are sent through unicasting mechanism as the end system knows the destination IP address.

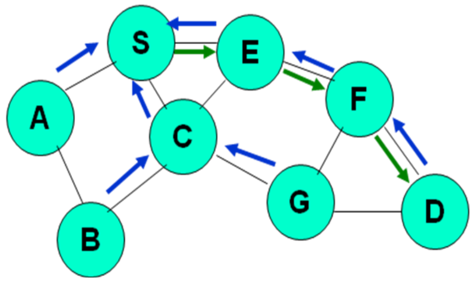


Fig: AODV path identification

### B. *AODV Table Terminologies and Modifications:*

AODV is a routing protocol, and it deals with route table management. Route table information must be kept even for short-lived routes, such are created to temporarily store reverse paths towards nodes originating RREQs. AODV uses the following fields with each route table entry:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid, Repairable, being repaired)
- Network Interface
- Hop Count (number of hops needed to reach Destination)
- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

## III. BASELINE LOCAL MONITORING (BLM):

Local monitoring is a collaborative detection strategy where a node monitors the control traffic going in and out of its neighbors. For a node, say α, to be able to watch a node, say N2, α must be a neighbor of both N2 and the previous hop from N2, say N1. Then α can be called as guard node for N2 over the link N1□N2 and use the notation R(N) to denote the set of all nodes that are within the radio range of node N and G(N1, N2) to denote the set of all guard nodes for N2 over a link N1 →N2. Formally, G(N1, N2 ) = R(N1)∩ R(N2 ) − N2 , where N ∈ R(N ) .

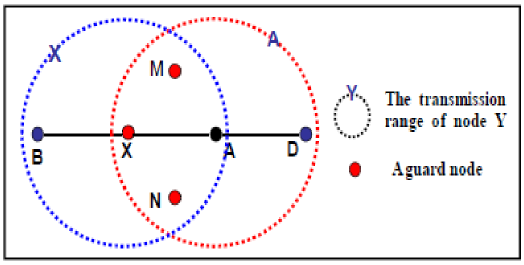


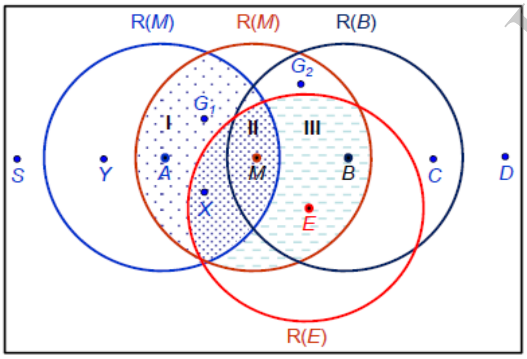
Fig: Baseline Local Monitoring overview

Information from each packet sent from X to A is saved in a watch buffer at each guard. The guards expect that A will forward the packet toward the ultimate destination, unless A is itself the destination. Each entry in the watch buffer is time stamped with a time threshold, τ, by which A must forward the packet. Each packet forwarded by A with X as a previous hop is checked for the corresponding information in the watch buffer. The check can be to verify if the packet is fabricated or duplicated, corrupted, dropped or delayed.

A malicious counter MalC(i,j) is maintained at each guard node, i, for a node, j, at the receiving end of each link that i is monitored. Counter is incremented for any malicious activity of j detected by i. The increment to counter depends on the nature of the malicious activity. When the value in the counter value maintained by a guard node i for node j crosses a threshold rate, node i revokes j from its neighbor list (called direct isolation) and sends to each neighbor of j, an authenticated alert message indicating j is a suspected malicious node. When a neighbor Ni gets the alert, it verifies the authenticity of the alert message. When Ni gets enough alert messages about j, it marks the status of j as revoked (called indirect isolation). The notion of enough number of alerts is quantified by the detection confidence index γ. Each node maintains a memory of nodes that it has revoked through a local blacklist so that a malicious node cannot come back to its neighborhood and claim to be blameless. This constitutes local isolation of a malicious node by its current neighbors.

## IV. SYSTEM DESIGN WITH BLM

The required change to the basic version of AODV is to enable the guards to build the necessary knowledge for detecting the misrouting attack. The idea behind the solution is that during route establishment, when the relation about which node to forward a packet between a given source-destination pair is determined, this information is broadcast by a neighbor to the guards which will be responsible for monitoring the node.



To collect the next-hop identity information, the forwarder of the Request (REQ) attaches the previous two hops to the REQ packet header. Let the previous hop of M be A for a route from source S to destination D, and the next hop from M be B. When M broadcasts the REQ received from A, it includes the identity of A and its own identity (M) in the REQ header <S, D, REQ_id, A, M>.

When B and the other neighbors of M get the REQ from M, they keep in a Verification Table (VT) <S, D, REQ_id, A, M, -> (last field is currently blank). When B broadcasts the REQ, the common neighbors of M and B update their VT to include B <S, D, REQ_id, A, M, B>. When B receives a REP to be relayed to M, it includes in that REP the identity of the node that M needs to relay the REP to, which is A in this example. Therefore, all the guards of M now know that M not only needs to forward the REP but also that it should forward it to A and not any other neighbor. Therefore, two tasks have been added to the functionality of the guards in monitoring the REP packets. First, the guard G of a node N verifies that N forwards the REP to the correct next-hop. In the example above, G2 verifies that M forwards the REP to A. Second, G verifies that N has updated the forwarded REP header correctly. In the example shown above, G2 verifies that when the input packet to M from B is <REP, S, D, REQ_id, C, B, M>, then the output packet from M should be <REP, S, D, REQ_id, B, M, A>. Thus M and its guards over the link B->M know that the next-hop is A from the information built in the VT table during the REQ flooding.

## V. CONCLUSION

Specifically, basic local monitoring (BLM) based detection cannot detect these attacks. Additionally, it will cause a legitimate node to be accused. Local monitoring fails in detecting the non-legitimate node and hence an additional activity is performed in the node (in transmission) and guard node. This scheme increases the deduction of the non-legitimate node than the local monitoring.

The non-legitimate node identity alert is send to the sender side and an alternative path suggestion is choose by the sender and the packets are re-transmitted. AODV is used for transmission of packets and efficiency of transmission can be increased by using R-AODV routing protocol. The ratio of packet sent becomes higher than the normal transmission with local monitoring.

## 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] Isha Khalil, S. Bagchi, and N. Shroff, “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks,” Proc. Int’l Conf. Dependable Systems and Networks (DSN ’05), pp. 612-621, 2005.

[3] “The Network Simulator - ns-2,” http://www.isi.edu/nsnam/ns, 2011.

[4] Isha Khalil, S. Bagchi, and N. Shroff, “SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. 37th Ann. IEEE/IFIP Int’l Conf. Dependable Systems and Networks (DSN ’07), pp. 565-574, June 2007.

[5] Isha 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 Comm. Networks (SecureComm ’08), http://doi.acm.org/10.1145/1460877. 1460913, 2008.

[6] Harsh pratap singh, sanjeev Sharma “Guard against cooperative black hole attack in Mobile Ad-Hoc Network” International Journal of Engineering Science and Technology (IJEST).

[7] C. Perkins, E. Belding-Royer “Ad hoc on-Demand Distance Vector (AODV) Routing”, RFC 3561, July 2003.