Exploring Mitigation Strategies for Common MANET Network Layer Attacks

Cameron Oakley

School of Computing and Design, California State University Monterey Bay, Seaside, California

Abstract

Mobile Ad-hoc Networks (MANETs) differ from traditional network infrastructures in terms of their data routing and the absence of a centralized authority for device authentication. MANETs have a key feature where the nodes regularly update their routing tables to keep up with changes occurring in the network. The exchange of information in this context relies on trust between the nodes, so each node must assume that its neighboring nodes are responding with accurate information. The level of trust needed in a MANET creates a security vulnerability that can be exploited by malicious actors.

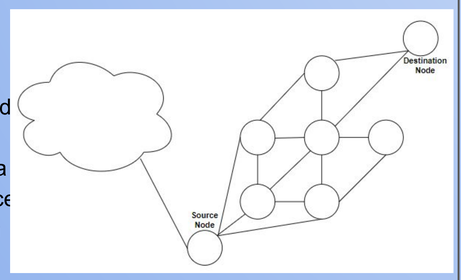
The focus of this work is to examine network layer attacks, such as Blackhole and Cooperative Blackhole, that threaten the stability and reliability of the network by disrupting the communications between nodes within a MANET.

Background

Blackholes - have legitimate use cases. ISPs route known spam addresses or ranges to a Blackhole which drops all the packets. Additionally, it can be used to prevent DoS attacks.
Node - act as an end device generating requests such as a smartphones or smart cars, and as a router in which they forward requests and responses.
Source node - the origin node which creates a request and sends it off into the network.
Destination node - the final destination of a request. Intermediate nodes forward a request until it reaches the Destination Node.
ACK - signifies OK data transfer sent from next in line node to node which forwarded the request.
Trusted Node (TN) - nodes that we have successfully communicated with reliably at some point.
Malicious Node (MN) - nodes that disrupt legitimate communications. In the case of this paper, MNs drop packets as they receive them.

MANET Architecture

Mobile Nodes: Nodes can move freely which changes the network topology.
Self-Sustaining Network: Nodes update their routing tables as the network changes.
Multiple Roles: Nodes act as an end device and as a router.
No Central Authority: Opposed to a traditional topology, there is no device facilitating communications between nodes.

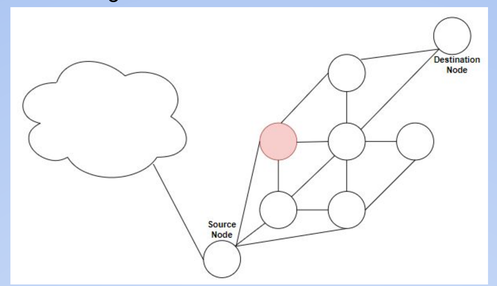


How can we get a request from the **Source Node** to the **Destination Node**?

Route Request: If a node does not have an entry for the Destination Node then broadcast a RREQ message to its neighbors. Neighbors repeat broadcast if needed.
Route Reply: If a node knows a path to the Destination Node, then they send a RREP message back to the node that forwarded the request.
Key Features: Intermediary nodes will update their routing tables upon receiving RREP message. Additionally, The Source Node determines which RREP has the "best" known path to the Destination Node via RREP Messages it receives.

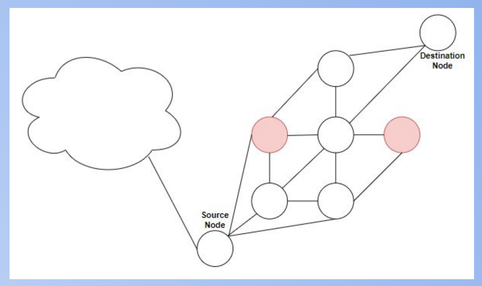
Blackhole Attack

A single malicious node in the MANET.



Cooperative Blackhole Attack

More than one malicious nodes in the MANET.



Process of sending a request from the **Source Node** to the **Destination Node** with intermediary MNs:

1. The Source Node doesn't know the path to the Destination Node, so a RREQ message is broadcasted to all of its neighbors.
2. If needed, it's neighbors broadcast the message further upstream.
3. A Malicious Node receives this RREQ message and responds with a false RREP message.
4. In this RREP message, the Malicious Node will declare itself the fastest path to the Destination Node.
5. From here, the Source Node will send the request to which the Malicious Node will drop it.

Mitigation Techniques

Sequence Number Thresholding: Set a sequence number threshold when sending false packets to the Destination Node. In this approach, the sequence number of the false packet will be incremented by one at each intermediary node visited. When the Source Node gets the response, if the response sequence number is higher than the threshold, then we can assume the path is unreliable.
Extended Data Routing Information (eDRI): Past and current TN information is stored in a table. Nodes that are new to the network should not be trusted. Nodes will spontaneously send false packets to untrusted nodes in order to determine if they are malicious or not. The eDRI table is continuously audited with changes occurring in the network.
Baiting Malicious Nodes: Broadcast a false packet addressed to a fake Source Node address. TNs would understand the Source Node address isn't real. Given a MN's behavior to respond to any broadcast it is baited and singled out. The TNs declare the MN as untrusted.
2ACK: These approaches typically involve sending an acknowledgment message non-traditionally. As a request is forwarded upstream to the Destination Node, acknowledgement messages are sent downstream to a node two hops away. So, when forwarding a request a node will expect to get an acknowledgement message back from the node 2 hops away. If no acknowledgement message comes back we can assume that the intermediate node dropped the request.
Trust-based Schemes: These approaches typically involve assigning a trust value to nodes within the network. Nodes will listen to the network and will monitor the packets sent to neighboring nodes. If a neighboring node drops packets then it's trust value is lowered. When it comes time to send or forward a request then the neighboring node with the highest trust value is chosen for forwarding.

Proposed Directions

Finding Trusted Nodes: Most researchers tend to be in accordance that a table for TNs is needed. In one proposal a TN table was used to store information about previously and current TNs. Storing information for all trusted nodes could be resource demanding, not only in terms of storage but the time for retrieving of information. The more nodes we have in our table the more routing overhead there will be. A worthwhile approach would be to drop old TN entries and query neighboring nodes in the event an unrecognized node is found.
Trust-based scheme: A trust-based approach could be effective for a TN table. When encountering an unrecognized node, neighboring nodes can be queried to determine if the unrecognized node is trustworthy. If found trustworthy, an entry will be created and it will be assigned a default trust value and subsequently monitored. Otherwise, if the node is found to be untrustworthy, it can be associated with a lower trust value. This approach may result in additional steps to verify the trustworthiness of unknown nodes, but it can improve the overall accuracy of trust assignments.
Finding Malicious Nodes: Using false packets to bait a Malicious Node is a unique approach. If our TN table has entries with low values, we can forward the nodes false packets that are originating from a false address. If a RREP message is received we associate the node with a low trust value as we now consider them to be a MN. This approach wouldn't overload the network with broadcast messages as it is being sent directly to suspicious neighboring nodes.

Acknowledgements

Special thanks to Dr. Sam Ogden and Dr. Paige Wiesskirch.

References

Dorri, A. (2016, March 23). *An Edri-based approach for detecting and eliminating cooperative black hole nodes in manet - wireless networks.* SpringerLink. Retrieved April 17, 2023, from https://link.springer.com/article/10.1007/s11276-016-1251-x

Gurung, S., & Chauhan, S. (2019, February 27). A survey of black-hole attack mitigation techniques in manet: Merits, drawbacks, and suitability - wireless networks. SpringerLink. Retrieved April 17, 2023, from https://link.springer.com/article/10.1007/s11276-019-01966-z

Yasin, A., & Abu Zant, M. (2018, September 6). *Detecting and isolating black-hole attacks in manet using timer based baited technique*. Wireless Communications and Mobile Computing. Retrieved April 17, 2023, from https://www.hindawi.com/journals/wcmc/2018/9812135/