



Stealth Attacks on Ad-Hoc Wireless Networks

Authors: Markus Jakobsson, Susanne Wetzel, Bulent Yener

presented by
Natthapol Pongthaiapat



Outlines

- Introduction
- Goal & Contribution
- Model & Assumption
- Operation
- Building Blocks for Attacks
- Attacks
- Prevention Mechanisms
- Conclusion



Introduction

- Large increase in inter-networking
- Reduction in Throughput, DoS
- Powerful attackers - high costs and high visibility (likely to get traced and busted)
- Skilled attackers - low costs and visibility (Stealth Attacks)




Stealth Attacks

- Two types of stealth attacks
- Network Disconnection - Partition (or DoS)
- Traffic Hijacking
 - Routing Modification
 - Traffic Analysis



Weapons

- Impersonate
 - introduction of packets with stated originators
- Lie
 - propagate incorrect information, such as bogus routing table
- Overloading

 Large amount of messages are dumped into one node causing DoS.

Goal & Contribution

- To further understanding of threats to routers by elaborating on attacks (details in how attacks can be perpetrated, categorize the techniques)
- Secure Protocol Design to protect routing information against the stealth attacks
- Proposed reputation based control (techniques used to evaluate good or bad routers) and message authentication which is light weight and do not require the use of a central Public Key Infrastructure.



Model & Assumption

- Concentrate on ad-hoc networks with mobility.
- As mobility increases, the distinction between locally and remotely mounted attacks disappears, mobility allows a modification of the routing table by simply moving into victim transmission range.
- Mobility helps disperse the information of which the attackers aim to advertise.



Model & Assumption

- There are two types of participants
 - Honest Participants
 - Cheaters (all nodes that do not behave correctly including nodes suffering from benevolent failures)
 - All cheaters are controlled by the attackers
- Two Power Classes
 - inexhaustible
 - limited power budget



Model & Assumption

- Three modes of operation depending on power level
 - Altruistic mode (charged), the router is in promiscuous state and performs any properly performed requests relating to routing
 - Egotistic mode (reduced), the router performs actions only directly benefits its transmission of packets.
 - Dead (exhausted power)



Operation

- Link Layer
 - Based on 802.11
 - Point Coordination Protocol (PCP)
 - Distributed Coordination Protocol (DCP) with CSMA/CA
 - Two way handshake
 - RTS \leftrightarrow CTS
 - ACK



Operation

- Network Layer
 - Proactive routing protocols
 - nodes maintain a connectivity graph by exchanging routing tables regardless of whether there is demand for routing to every entity in the table.



Dijkstra's shortest path, Distance Vector



Operation

- Reactive routing protocols
 - routing information is obtained when there is a demand to send traffic to a particular destination.
 - Route discovery is usually done by flooding, routing information is stored locally (caching), but may not be communicated to others unless requested.
 - Each node learns the routing information from the routing information from the route discovery process.



Operation

- Dynamic Source Routing (DSR), Ad-Hoc On-Demand Distance Vector Routing (AODV), Zone Routing Protocols (ZRP).
- An attacker can easily overflow routing caches or tables with incorrect routes to replace the correct ones to the victim.



Building Blocks for Attacks

- Remove or add entries from/to routing tables.
- Removing an entry using impersonate
 - In proactive protocols, by taking an advantage of routing updates, an attacker can impersonate a neighbor N of victim V, and claim that victim V is down.
 - In reactive protocols,
 - aim at route discovery process
 - two nodes involved, one makes a request, the other is on the requesting path.
 - The latter reply with route error message, all nodes between these two will believe that the former is unreachable and subsequently delete the corresponding route from their caches.



Building Blocks for Attacks



- Removing an entry without impersonation
 - In reactive protocols, an attacker can simply force the dropping of route discovery message from controlling node N_i in the route $N_1-N_2-...-N_i-...N_k-V$. The nodes in the path $N_1-N_2-...N_{i-1}$ will not discover the path.
 - In proactive, an attacker can imply attacks the routing table during the update process.



Building Blocks for Attacks



- Adding an entry using impersonation.
- Adding an entry without impersonate.
- Both use the same concept as removing an entry with/without impersonation. Instead of removing or dropping routing information, malicious routing (e.g., non-existing route) information is advertised during route update or route discovery reply .



Building Blocks for Attacks



- Jamming - generate traffic to collide with control messages for route discovery / update process
- Consuming power to change operation mode
 - Force power consumption on a victim, causing the victim to switch off from promiscuous mode.
 - Victim is no longer participate in routing, network is partitioned.
 - Using false link failure report causing unnecessary routing update (proactive protocols).
 - Broadcasting a route request from a remote location to a non-existing destination (reactive protocols).



Attacks



- Disconnection
 - Use previous described building blocks for attacks.
 - Route considerable amounts of traffic to the victims
 - forcing them to run out of power.
 - Perform a power attack on all known neighbors of the victim node.
 - Routing large amount of traffic causing traffic overload (insufficient bandwidth)
 - Removing/modifying victim routing information.



Attacks

- Throughput reduction
 - Disconnecting a large number of nodes will result in considerable reduction in throughput.
- Active Eavesdropping
 - Hijacking victim traffic
 - Corrupt routing tables of nodes on the victim communicating path
 - Force incoming/outgoing traffic to attacker control nodes by using false routing tables.



Prevention Mechanisms

- Use cryptographic authentication to prevent impersonation.
- Improve the resistance against stealth attacks.
- Full-Blown authentication is costly.



Prevention Mechanisms

- Sometimes, correct authentication of control messages does not correspond to correctness of the control information.
- It is hard to verify who is exactly and who is not an honest server.
- To solve the above problem, each router can keep (and possibly exchange) reputation based information.
- The reputation based information can be used to resolve conflicting information, and to determine what control messages to handle an act on.



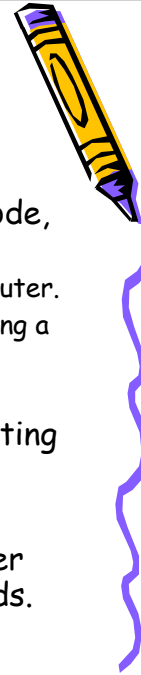
Prevention Mechanisms

- Although the speed is reduced, the node is less prone to the attacks.
- Drawn from real life, by constantly learning and observing routing traffics, each router may keep "reputation tables or caches" listing nodes they trust.
- A router may also request reputation tables when it moves into a new network neighborhood.



Prevention Mechanisms

- To determine the reliability of a particular node, two heuristics are proposed by observing,
 - the average number of retransmission to a given router.
 - the number of successful exchanges of data involving a given router.
- Keep the records of router discovery and routing update and credit to the involved router.
- Judge the reliability of a recommending router by the reliability of the routers it recommends.



Prevention Mechanisms

- Use light weight authentication mechanisms to prevent the overloading attacks.
- Use Message Authentication Codes instead of Digital Signatures (the goal is not to establish exactly who originates the information but rather to recognize the same entity in consecutive iterations)
- Integrity of routing tables is protected.
- Reputation based control is not a full remedy for security problem, it just makes the job become very harder for attackers. It is still possible to destroy the reputation.



Prevention Mechanisms

- To prevent attackers to remove victim routing tables, a certain degree of inertia in terms of when entries are dropped from routing table can be added.
- The exact degree of inertia depends on the degree of interconnectedness of the trusted nodes.
- Routing can be strengthened to make it resistant against the attacks.



Conclusion

- Reputation based control is introduced to lessen the degree of vulnerability of ad-hoc network against malicious attacks (remove/add false routing information).
- Protection against one type of attacks usually weakens the network against a second type of attacks.
- Finding the balance is extremely difficult.

