Course: Advanced Networked Systems Security
Lecturer: Panos Papadimitratos
Scribed by: bastianf@kth.se

Lecture 3 – Secure Routing

Definitions

***Definition* Mobile Ad Hoc Network (MANET)**
Mobile Ad Hoc Network (MANET) is a self-organising network of wireless nodes without any central networking infrastructure.

***Definition* Secure routing problem**
The *secure routing problem* is the problem of successfully routing packets (between a source and a destination node) in a MANET in the presence of one or more malicious nodes.

Previously proposed solutions to the secure routing problem

Spy on next hop node: Nodes work in promiscuous mode in order to overhear traffic sent by the next hop node. If the packet has been altered, a report is created and the rating of the next hop node is decreased. The path metric then becomes the average of the ratings of the nodes in the path. The path with the highest metric is chosen.
Problem: A situation can arise where many nodes are falsely detected as misbehaving. The metric construction might to a choice of path containing a malicious node. No way of validating correctness of reports.

Routing with incentive: Provide incentive for nodes to comply with the protocol, e.g. using a cryptocurrency[1] or a TRSM. Each intermediate node purchases the packet from the predecessor and sells it to the next hop node.
Problem: Requires a PKI. Nodes could flood the network with packets destined to non-existing nodes to earn money. High computational overhead.

Secure Message Transmission (SMT): Determine a set of paths to the destination node. Split the message to send into N pieces using an M out of N scheme[2]. The original message can be reconstructed at the destination node if at least M pieces was received correctly. When the original message has been reconstructed, the destination node sends an acknowledgment (using a 1 out of N scheme) back to the source node. The acknowledgement contains information about which pieces were received, thus giving information about which routes are working. The rest of the data is then sent over the working routes.
Problem: Limited protection against use of compromised topological information. May be combined with SRP described below[1].

Secure Routing Protocol (SRP)

SRP works on top of the IP layer. Requires security association (SA) established between source and destination node. Assuming bi-directional links and nodes working in promiscuous mode[1]. The purpose of SRP is to perform *route discovery*.

[1] The original paper does not mention anything about cryptocurrency.
[2] See https://en.wikipedia.org/wiki/Secret_sharing

Course: Advanced Networked Systems Security
Lecturer: Panos Papadimitratos
Scribed by: bastianf@kth.se

Route request packet

SRP Header			Route
ID	SN	MAC	$n_1, n_2 \ldots n_k$

Broadly speaking, the protocol works as follows:

1. The source node starts by sending a route request packet to the destination node.
2. Intermediary nodes appends their IP address in the route and relays the packet to the next hop node.
3. When the destination node D receives the packet, it performs the following steps:
    a. The authenticity of the packet is checked using the SA and the MAC.
    b. The sequence number (SN) is checked.
    c. A response packet is sent to all of D:s neighbours. The response packet (protected and authenticated by a MAC) and is sent over the reverse path n_k, $n_{k-1} \ldots n_1$.

SRT guarantees that discovered routes does not contain any loops. Furthermore, SRT also guarantees that each of the intermediary nodes has been up at some point between the time a route request packet was sent and a response was received. SRT is also accurate, in the sense that the route metric computed by the source node is within a constant of the actual metric[2].

Fault detection in SMP

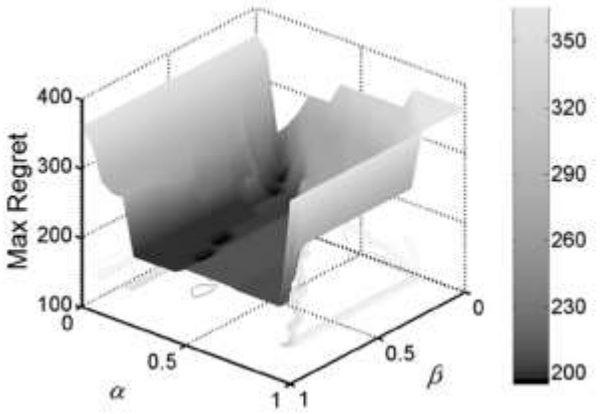
Each path in SMP is associated with a rating R between R_{min} and R_{max}. The rating is updated using the following formula

$R_{new} = \max(R_{old} - a, R_{min})$ if packet loss
$R_{new} = \min(R_{old} + b, R_{max})$ otherwise

a and b are constants between 0 and R_{max}. It can be shown that the fraction of discarded packets is at most $\frac{b}{a+b}$[3].

Selection of M and N

If we split a message into N parts and M parts are required to recover the message, we define $R(M, N)$ as the probability of successfully recovering the message. Let P_{GOAL} denote the smallest acceptable probability of recovery, and r_{GOAL} the highest acceptable transmission overhead.



1 Given that we want to minimize the maximum possible packet loss, we should choose a and b randomly such that the corresponding max regret is low[3].

Paths to the destination are sorted based on 1) Rating 2) Survival probability and 3) Hop length[3]. Then determine N and M based on the following objectives:

1. Minimize N such that R(M, N) is at least equal to P_{GOAL}
2. Minimize the redundancy without affecting the choice of N
3. Maximise redundancy without exceeding r_{GOAL}

Castor

Castor is a secure routing scheme without route discovery. Castor is scalable, since no routes are stored in the packages being transmitted, and each node only needs to remember its neighbours.

Castor uses two types of packages, a payload packet and an acknowledgement. The payload packet consists of source, destination, a flow id, a flow authenticator, a packet id, payload and an encrypted ACK authenticator. The ACK authenticator is a random number. The packet id is the hash of the ACK authenticator.

When an intermediary node receives a packet, it checks whether the packet belongs to the flow using the packet id and a Merkle hash tree[3] with the hashes of the packet ids as leaves and the flow id as root. The Merkle Proof is the flow authenticator.

At the destination, the packet id b_k is checked against the decrypted hash of the ACK authenticator $h(Decrypt(e_k))$. Also, the integrity of the payload is checked. If everything looks good, an acknowledgement is sent back to the source node. When the source receives the ACK it checks whether the hash of the ACK identifier $h(a_k)$ matches any stored packet id b_k[4].

References

[1] P. Papadimitratos and Z.J. Haas. "Secure Routing for Mobile Ad hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (SCS CNDS), San Antonio, TX, USA, January 2002

[2] P. Papadimitratos, Z.J. Haas, and J.-P. Hubaux, "How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET," IEEE-CS BroadNets 2006, San Jose, CA, USA, October 2006

[3] P. Papadimitratos and Z.J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Security in Wireless Ad Hoc Networks, February 2006

[4] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable Secure Routing for Ad-hoc Networks," *IEEE Conference on Computer Communications (IEEE INFOCOM)*, San Diego, CA, March 2010

[3] Read more here: https://blog.ethereum.org/2014/08/16/secret-sharing-erasure-coding-guide-aspiring-dropbox-decentralizer/