AnoMul: An Anonymous Multicast Routing Protocol For Mobile Ad Hoc Networks

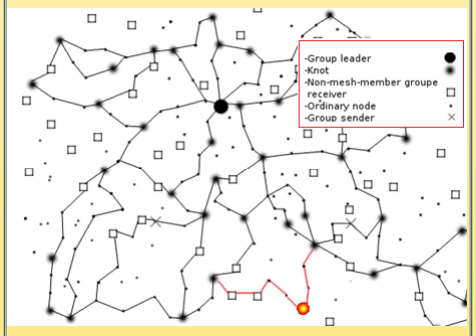
Somayeh Taheri, Dieter Hogrefe
Institute for Informatics-Göttingen, Germany
taheri@informatik.uni-goettingen.de

Introduction

Introduction: Mobile ad hoc networks (MANETs) are self-configuring networks of mobile devices without need to any existing infrastructure, suitable for areas where rapid network reconfiguration is needed such as search and rescue operation, battle field communication and conferences. The lack of a trusted centralized authority, limited resources, mobility and the broadcast nature of the wireless links make these networks very susceptible to security and privacy threats.
Anonymity is still a challenging issue in mobile ad hoc networks (MANETs). Specially although operating as groups is required by many applications, there is only a little work on anonymous multicast routing protocols. In this work an Anonymous Multicast routing protocol for MANETs (AnoMul) is proposed. AnoMul is a mesh based multicast routing in which we extend the idea of identification free routing proposed by Kong et al. in ANODR protocol to multicast routing.

AnoMul

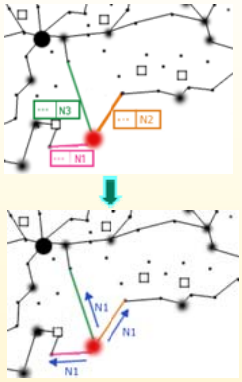
Mesh Construction: We exploit the identification-free route discovery approach, introduced by J. Kong and X. Hong in [1], to discover the routes in AnoMul. We rename the RREO and RREP packets to JREO and JREP indicating Join REQuest and RERly messages (of the same format as in ANODR). When a group receiver decides to join mesh, it broadcasts a JREQ message and waits to receive a JREP from another group member which is already joint to the mesh (called a knot). Any node having data packets to send to the group will join the mesh in the same way, and then will send data packets through its connections to the mesh.
Mesh leader selection: The first node joining the mesh is the mesh leader.



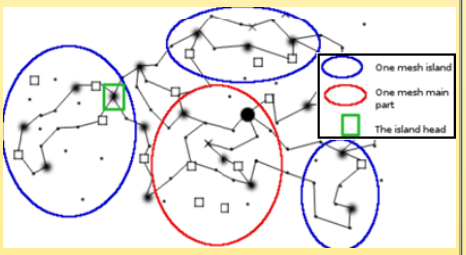
The knots will forward data packets through their connections to the whole mesh.
Due to using ANODR for route discovery a link pseudonym is shared between any two neighbours on routes used as a key to re-encrypt data packets later on.

AnoMul (cont.)

Multiple forwarding issue: since the route pseudonyms shared by any knot with its neighbour knots are different, it would need to send the data packets several times
➢**Solution:** Route pseudonym unification (sharing the first shared pseudonym with every new connection as well)



Mesh Maintenance: The mesh leader sends periodic packets to the mesh to let the knots know if they are still connected to the mesh. When a mesh receiver does not receive the periodic messages for a long time it realizes that most likely it has lost all connections to the mesh leader
➢**Mesh Maintenance optimization:**
We refer to any part of the mesh which includes the mesh leader as a main part, and any part of the mesh which does not include the leader as a mesh island. If an island is disconnected from the mesh because one knot has lost its connections to the mesh's main part (island head) then we use an efficient mechanism to reconnect the island. The idea is to find a new route to the mesh just by the island's head, not by every knot in the island.



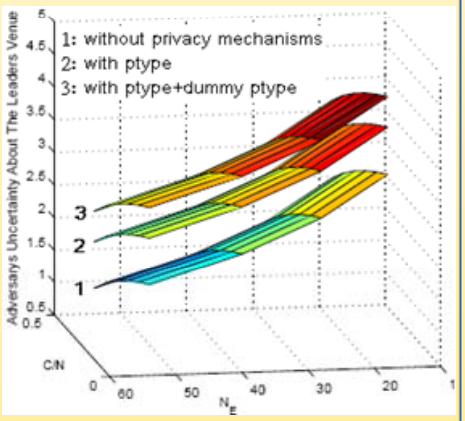
Group Sender Privacy:
➢ To form a group of semi-senders for each sender formed by a number of knots
whose behavior is just like the real sender. The real sender chooses them among its neighbor knots by sending a message to them. Then each data packet is sent to the mesh randomly by one of them to provide sender location privacy.

Group Leader Privacy:
I. Protected type mechanism (Ptype):
Ptype is used as the unified message type for

AnoMul (cont.)

the whole message types sent among knots over the discovered routes such as periodic leader messages, route pseudonym unification messages, data packets, etc. The Ptype messages are encrypted with the route pseudonyms and if the node receiving a Ptype message can find the route pseudonym of the message in its routing table, then it has to proceed the message no matter of which type the message is. When this mechanism is used the adversary can not distinguish leader messages for sure.
II. Using dummy Ptype messages

➢The attack scenario against leader location privacy:
Adversarial nodes divide the network into N_E cells and one eavesdropping node listens for Ptype message in each cell. In this attack the adversary will consider the nodes who forward a Ptype message earlier than the others (in each period) to be closer to the leader and uses this information to find the leader's location. The following figure shows how under this attack scenario the adversary's uncertainty about the location of the mesh leader increases when Ptype mechanism and dummy Ptype messages are used. (C=number of captured nodes; N=network size)
We suppose that the adversary has the ability to capture some network nodes.



Conclusion

In this proposal we described some ideas of an anonymous multicast routing protocol for MANETs, AnoMul. We will evaluate AnoMul's performance and publish a detailed version of this work in future.

References: [1] Jiejun Kong and Xiaoyan Hong. Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, New York, NY, USA, 2003.