Secure Multi-hop Ad Hoc Connectivity to Fixed Networks

Frank Egle, Tim Leinmüller, Michael Schäfer and Elmar Schoch
DaimlerChrysler AG, Research Vehicle IT and Services,
{Frank.Egle|Tim.Leinmueller|Michael.F.Schaefer|Elmar.Schoch}@DaimlerChrysler.com

***Abstract*— Mobile multi-hop ad hoc networks are a cost-effective way to internetwork mobile nodes without relying on any infrastructure. Nevertheless certain applications require access to a fixed infrastructure or larger networks like the Internet.**

Access to fixed infrastructure from ad-hoc networks is possible through gateway stations, but to create seamless connectivity, an entire area would have to be equipped with a high number of gateway stations, leading to very high costs.

Beneath the quite simple solution, direct access of mobile nodes to fixed infrastructures, there is another possibility to connect to fixed networks. Multi-hop routing via intermediate nodes enables moving nodes to reach gateways, which are outside of the moving nodes' proper radio range. This method has the potential to lead to a much lower number of gateways required to offer seamless connectivity to a fixed infrastructure. However, due to the properties of the multi-hop access channel there are new security issues arising. For instance, there have to be mechanisms in place in order to prevent unauthorized usage of gateways and the ad-hoc network, to detect malicious nodes, to prevent eavesdropping, to manage the mobility of the nodes and last but not least to ensure the privacy of the user.

Our research presents a solution for the secure network attachment of multi-hop ad hoc networks to a fixed infrastructure. Our solution is able to limit the traffic in the ad-hoc network heading towards the gateway to authorized traffic and management data. In addition, it is able to ensure the privacy of the nodes communicating with the gateway. Traffic is always controlled and authorized by the gateway. Additionally encryption protects the payload of the communication.

I. Introduction

The general idea of multi-hop ad hoc access to public networks is to provide low cost access to fixed (operator provided) networks in areas without deployed fixed infrastructure gateways. A typical example would be an automotive scenario as shown in Figure 1, where wireless connectivity between vehicles is used to access roadside Internet gateways [1].

In Figure 1, only vehicle $V2$ has a connection to an infrastructure access AP. At the same time, $V2$ has ad hoc connectivity to nodes $V1$ and $V3$, as well as to $V4$ via $V3$. Assuming that $V4$ wants to access the infrastructure, it has to use the connection provided by $V2$ and $V3$.

Whereas in other multi-hop scenarios, intermediate nodes belong to a single entity (or administrative domain), in our scenario these nodes belong to different owners and they do not necessarily have pre-established security associations. Intermediate nodes are at the same time other users' "end nodes", thus this implies that they are supposed to move frequently, in a vehicular scenario even with high velocity.

During the remainder of this paper, we use the following assumptions. Nodes belong to different owners and do not have pre-configured security associations amongst each others. Nodes use temporary cryptographic identifiers in the ad hoc network in order to guarantee a certain level of privacy (i.e. to prevent traceability). Toward the fixed network, nodes identify themselves with their Node ID. Nodes move with high velocity in respect to each other, thus we consider the usage of position dependent routing, see [2] and [3]. Gateways have an operator dependent, cryptographic identifier (Gateway ID). Nodes know these identifiers or are at least capable of verifying them (i.e. using a pre-installed global root certificate of the operators).

The remainder of this paper is organized as follows. The next section II clarifies the problem statement, followed by the proposed technical solution in section III. Section IV elaborates on the used security concepts and provides a brief architecture evaluation. Finally section V summarizes this paper's main achievements and section sec:conclusion concludes the paper.

II. Problem Statement

When realizing a scenario as depicted above, several constraints have to be respected. To prevent traceability and other privacy issues the node identity (Node ID) or

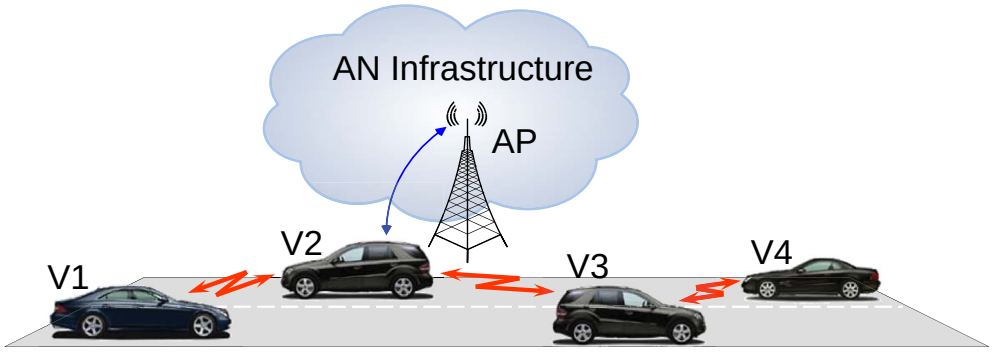

Fig. 1. Example Scenario

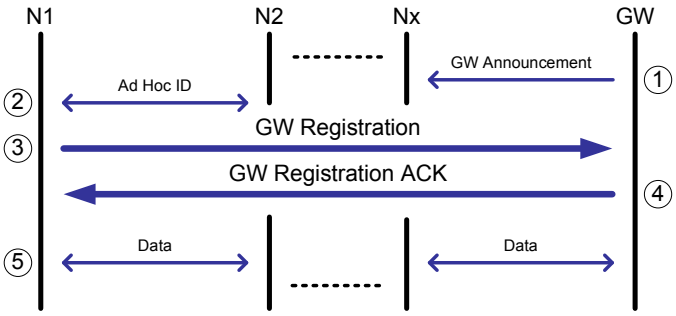

Fig. 2. Data Flow

identifier of an ad hoc node should not be revealed to other ad hoc nodes on any network layer. On the other hand, the ad hoc network should assure that forwarded traffic is limited to authorized communication, as well as that intermediate nodes can not be held responsible or made liable for relayed traffic.

III. Proposed Technical Solutions

In order to meet the previously introduced requirements, we advocate a solution as depicted in Figure 2.

This solution can be divided into the following five segments:

1) Gateway Announcement: Gateways periodically announce their presence to ad hoc nodes. These advertisements include the cryptographically verifiable ID of the gateway (Gateway ID), which also identifies the gateway as such. These gateway announcements are propagated through multiple nodes, thous reaching nodes not in direct visibility of the gateway.
2) Ad Hoc ID exchange between adjacent ad hoc nodes. Upon discovery of a new neighbor, ad hoc nodes exchange their temporary identifiers. This is required to unambiguously address neighbors afterwards during communication, without revealing the ”real” Node ID in the ad hoc network.
3) Gateway Registration: If ad hoc nodes want to attach to a fixed network via a gateway, they send an encrypted registration message addressed to the selected gateway, which is then forwarded by intermediate nodes until it reaches the gateway. Such a registration message contains the encrypted Node ID, by which the gateway is able to determine, whether the node is allowed to access the fixed network infrastructure. This is the only message type that has to be relayed by intermediate nodes, without authorization by the gateway. Furthermore the throughput of such registration message could be limited in the network.
4) Gateway Registration Acknowledgment: After verifying the Node ID against the access policy of the gateway’s domain, the gateway issues a registration acknowledgment. This acknowledgment contains a certificate bound to the ad hoc node’s current temporary identifier. The validity of this certificate is limited in time and verifiable by all intermediate nodes.
5) Data communication with nodes inside the fixed network: After the reception of the registration acknowledgment, the ad hoc network node is able to communicate with other nodes within the infrastructure via the gateway. To link the encrypted traffic with the gateway registration and the current ad hoc ID, the node attaches the Gateway provided certificate to the packets. This enables intermediate nodes to differentiate between gateway authenticated traffic and non-authorized traffic and consequently to forward only legitimate traffic. Furthermore, this concept is adapted to changing forwarding paths within the communication chain

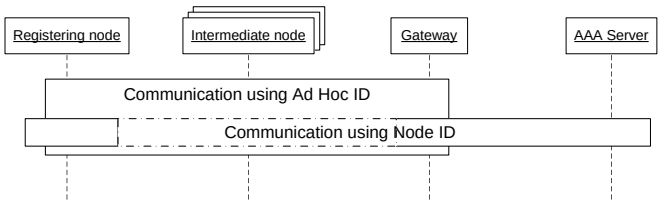

Fig. 3. Visibility of Node ID

to the gateway, as they are expected in highly dynamic ad hoc networks.

IV. Security Concepts and Architecture Evaluation

A. General Concepts

As stated before, one critical requirement for the ad hoc network environment is not to reveal the Node ID to other nodes of the ad hoc network. Only the gateway needs to be able to access the Node ID. Therefore, a separate Ad Hoc ID for usage in the ad hoc network environment is introduced. That means that addressing within the ad hoc network is done only by the Ad Hoc ID.

As a consequence, if the network is to be used only by nodes with valid access credentials for the fixed infrastructure, the Ad Hoc ID has to be bound irreversible to the Node ID. This is achieved using asymmetric cryptography.

For the further sections, we use the following terminology:

K_{OP} = Operator Public Key
K_{OP}^{-1} = Operator Private Key
K_{GW} = Gateway Public Key
K_{GW}^{-1} = Gateway Private Key
K_{AH} = Ad Hoc Node Public Key
K_{AH}^{-1} = Ad Hoc Node Private Key
$\{abc\}_K$ = Encrypted data (abc) using key K
$h(abc)$ = Hashvalue of data (abc)

For reasons of efficiency, the public key of ad hoc network participants is used as its address simultaneously. As we will see in later sections, all packets traveling in the ad hoc network have to carry the public key of the original sender - therefore it is obvious to use the public key as address too. Initially involved entities have to be in possession of the following cryptographic material:

Operator: K_{OP} and K_{OP}^{-1}
Gateway: K_{GW} , K_{GW}^{-1} and $\{K_{GW}\}K_{OP}^{-1}$
Node: K_{AH} , K_{AH}^{-1} and K_{OP}

B. Gateway Announcement

To make passing nodes aware of the presence of an gateway, the gateway periodically broadcasts announcement messages. These messages are forwarded by receivers until a maximum hop count is reached. Alternatively, the validity of the gateway announcements may be limited by a geographic area. Besides the address of the Gateway itself (which is also its public key K_{GW}), the announcement messages carry an operator signature of this address. Therefore each node is able to verify that the source of an announcement is an official gateway. As consequence, receiving nodes acquire the following

- Availability of an gateway
- The public key of the gateway K_{GW} and
- corresponding operator signature $\{K_{GW}\}K_{OP}^{-1}$

C. Ad Hoc ID Exchange

For routing purposes and in order to support position dependent applications (which are not in the focus of this document), each node periodically broadcasts its position and its Ad Hoc ID. This is often called ”beaconing”, and is used in many geographic routing approaches. The difference to simple beaconing is that every beacon message is signed by $\{K_{AH}\}K_{AH}^{-1}$. This prevents potential attackers from impersonating arbitrary identities.

D. Gateway Registration and Acknowledgment

The security concept is designed to only allow forwarding of messages in two cases:

1) Either, the corresponding original sender of the packet is a registered node, i.e. the gateway has signed its Ad Hoc ID, the signature is carried by the packet and the original sender has signed the packet using its private key.
2) Or, the packet is a (signed) registration request.

If a node tries to send data, all forwarding nodes will approve the validity of the packet.

1) Node Sends Registration Message to Gateway: Because the registration packet itself cannot carry the gateway certification, that type of message must be forwarded by intermediate nodes to the gateway without approval. On the other hand, to prohibit unintended use of gateway registration messages, the number of forwarded registration messages from a distinct node may be restricted by time. At first, the node creates a packet containing

- the Ad Hoc ID/Public Key as sender identifier (i.e. K_{AH})
- the Node ID, encrypted with the public key of the addressed Gateway as payload (i.e. $\{AN\,ID\}K_{GW}$)

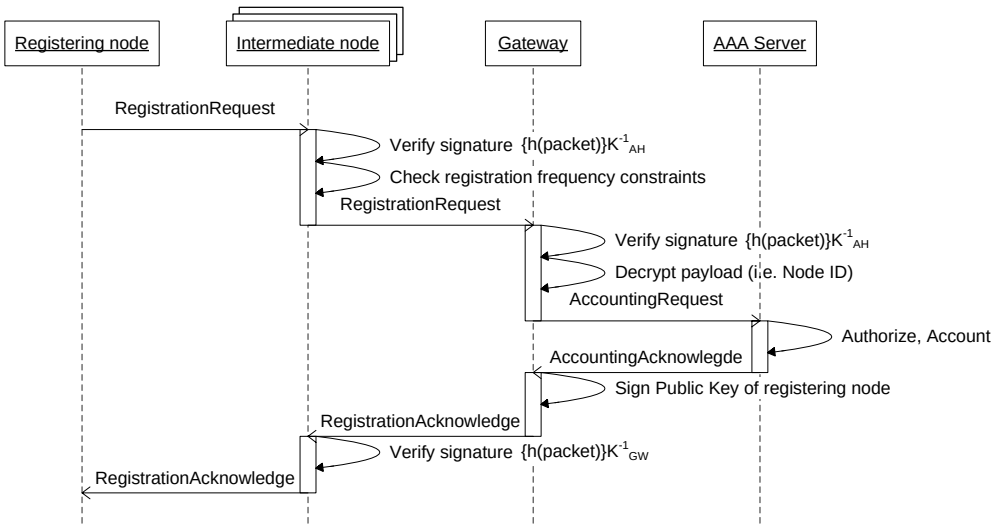

Fig. 4. Registration With a Gateway

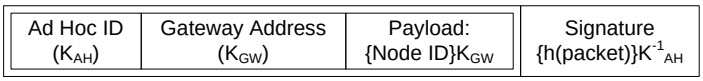

Fig. 5. Gateway Registration Packet

- a signature of the whole packet, created using the nodes' Private Key (i.e $\{packet\}K_{AH}^{-1}$)

The corresponding packet format is show in Figure 5. This design has several advantages:

1) Every relaying ad hoc node can associate registration packets uniquely to one node since the signature can only be created by the original node with the corresponding private key
2) The Node ID is not open to intermediate relaying nodes because it is encrypted by the original sender with the public key of the gateway, so only the gateway is able to decrypt the Node ID.

2) Gateway Sends Registration Acknowledge to Node: When a registration message reaches the gateway, AAA processes in the background network allow or decline the usage of the gateway for the corresponding node.

As response to the registration, the gateway sends a registration acknowledgment. The acknowledgment especially contains a certification ($\{KAH\}K_{GW}^{-1}$) of the node's Public Key/Ad hoc ID. This certification afterwards serves as approval of registration for relaying nodes.

The conceptual format of registration acknowledge messages is depicted in Figure 6.

The complete registration process with all involved instances and their related tasks is given in Figure 4.

E. Data Communication

After a successful completion of the registration process, the node is able to communicate with the fixed network via the ad hoc network and the gateway. With the certificate of approval added to every packet, relaying nodes now are able to verify that the gateway has registered the corresponding Ad Hoc ID.

Moreover, the signature of the packet also assures, that only the original node is the sender since the signature can only be created using the private key that corresponds to the nodes public key/Ad Hoc ID.

The conceptual format of a registered multi-hop data packet is depicted in Figure 7.

V. Summary of Results

The presented schemes achieve the following:

1) Authentication of ad hoc nodes: With the registration process being mandatory, every node in the ad hoc network has to register with the gateway before it is able to communicate both within the ad hoc network and the infrastructure network. Every relaying node is able to verify that the source of a packet is an authenticated node.
2) Integrity protection: Due to the fact that each packet has to be signed by its original sender, intermediate nodes cannot change the transported payload without being detected.

Fig. 6. Gateway Registration Acknowledge Packet

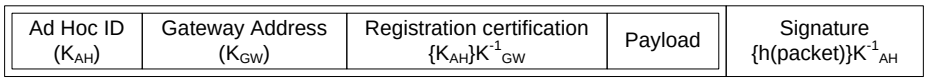

Fig. 7. Registered Multi-hop Data Packet

3) Node ID protection: Among ad hoc nodes, communication is based on the Ad Hoc ID. Therefore the Node ID is only visible to the infrastructure background network, especially to gateways and AAA servers.
4) Routing security: Concerning routing security, the signing mechanisms prevent a malicious node from being able to inject messages that are routed through the network unless it is registered with an gateway. Using useless registration requests to disturb the network is prevented by time constraints that are checked by relaying nodes.

VI. Conclusions

The proposed solution presents a method to securely connect a mobile multi-hop ad-hoc network to a fixed infrastructure, leveraging the extended connectivity of intermediate nodes. Our solution fulfills all our self-imposed security and privacy properties like limiting the traffic to authorized traffic, protecting node privacy, gateway-centric traffic access-control and accounting as well as payload encryption and integrity. At the same time the solution does not rely on any pre-established security associations between the nodes, aside from the global knowledge of the root public key of the operators.

In our ongoing research, we work on remaining open issues, such as improving security of the underlying position dependent routing, mechanisms to encourage node co-operation, as well as handover of established security associations.

Handover addresses two important aspects: The handover between two adjacent gateways as well as the ”handover” between two different Ad hoc IDs of the same node, which are changed regularly for privacy reasons.

Furthermore we will research if a variant of our proposed solution could also enhance the security of multi-hop unicast communication in the ad-hoc network and if concepts like onion routing could be integrated into the solution.

References

[1] M. Bechler, W. J. Franz, and L. Wolf, “Mobile Internet Access in FleetNet,” in *KiVS 2003*, Leipzig, Feb. 2003.
[2] M. Mauve, J. Widmer, and H. Hartenstein, “A survey on position-based routing in mobile ad-hoc networks,” *IEEE Network Magazine*, vol. 1, pp. 30–39, Dec. 2001.
[3] C. Maihöfer, R. Eberhardt, and E. Schoch, “CGGC: Cached greedy geocast,” in *Proc. 2nd Intl. Conference Wired/Wireless Internet Communications (WWIC 2004)*, ser. Lecture Notes in Computer Science, Frankfurt (Oder), Germany, Feb. 2004.