Scalable Revocation in Hybrid Ad Hoc Networks
The SHARL Scheme

Mona Holsve Ofigsbø
Department of Telematics, NTNU, Trondheim, Norway
Email: monaof@item.ntnu.no

Anne Marie Hegland¹, Pål Spilling², Øivind Kure³ and Leif Nilsen²
¹Kongsberg Defense and Aerospace, Billingstad, Norway
²Department of Informatics, UiO/Unik, Oslo, Norway
³Q2S, NTNU, Trondheim, Norway
Email: anne.marie@kongsberg.com, paal@unik.no, okure@q2s.ntnu.no and l_nilsen@unik.no

Abstract— The article proposes a simple, scalable and robust scheme for the distribution of revocation information in mobile ad hoc networks (MANETs). The scheme is intended for ad hoc networks with a planned origin, and where a common point of trust exists. Mobile ad hoc networks have limited available bandwidth. The revocation lists must therefore be specific to the network. They are established with the aid of trusted gateways reporting the identity of the nodes to a central trusted entity. To minimize overhead, the revocation lists are distributed along with the routing messages. In the articles we discuss how the scheme can be implemented in conjunction with the predominant routing protocols in ad hoc networks. The article also provides a detailed security analysis of the proposed protocols, partly based on the use of formal methods.

Index Terms—Management, ad hoc networks, revocation, routing protocols and formal method.

I. INTRODUCTION

Unilateral authentication of the routing messages enables the protection of the network layer. Possible solutions include symmetric message authentication codes and asymmetric (public key) schemes such as digital and identity-based [23] signatures. Symmetric schemes are efficient both regarding computational efficiency and bandwidth consumption. However, changes in group membership imply re-keying. This represents a threat to network availability. There is no guarantee that all nodes receive the new key in a timely manner. Although still challenging, the exclusion of specific nodes is easier with asymmetric schemes. A survey of key management schemes for the protection of routing information in ad hoc networks is found in [13].

In traditional public key schemes, a trusted entity signs certificates that bind public keys to IDs. In identity-based schemes, IDs, e.g., IP-addresses, serve as public keys. The corresponding private keys are derived by a trusted entity. In traditional public key schemes revocation refers to the invalidation of certificates. In identity-based schemes, IDs are revoked.

This paper focuses on revocation of certificates and IDs used to protect routing information in MANETs used in emergency and rescue operations. This means ad hoc networks with a planned origin, and where common points of trust exist, and pre-configuration is possible. Our MANET is connected with an internet through one or more gateways, a so-called hybrid MANET. Only authorized nodes are allowed to join the MANET. Exclusion of captured or malfunctioning nodes necessitates distribution of revocation information over the ad hoc network.

A number of methods for certificate revocation have been proposed [25][26][28]. Unfortunately, these are generally not very well suited for the mobile ad hoc environment. Crépeau and Davis [6] propose an accusation-based revocation scheme for ad hoc networks. Certificates are issued by an off-line certificate authority prior to network participation. All nodes monitor the behavior of the others. Accusations are posted if discrepancies from “good behavior” are detected. A certificate is revoked when a threshold number of accusations have been posted against one node. Any node is only allowed to post a single accusation against any other node.

The scheme offers limited robustness to varying network connectivity. The nodes are assumed to maintain both a common view of the number of nodes in the network and the behavior of these nodes, which is a strong requirement in ad hoc networks. Furthermore, a new node may lead to network congestion as the other nodes are supposed to send their certificates and profile
tables (listing their view of earlier accusations and revocations) to newcomers.

In [16], Jungels, Raya and Hubaux suggest a revocation scheme for vehicular ad hoc networks (VANETs). VANETs differ from MANETs in the sense that the nodes move along roads. The nodes communicate vehicle-to-vehicle or via base stations and fixed infrastructure available along the road. In each vehicle, the keys are stored in a tamper-proof device. On revocations, the CA residing in the fixed net sends a key-erase message to the tamper-proof device. If the device does not confirm the erasure of all its keys, the CA warn other neighbors by a revocation list sent through a side channel, e.g., a FM channel. The key erasure and warning messages demand infrastructure. If the vehicles are out of range of a base station, the nodes warn each other through accusations in a way similar to the accusation based method of Crépeau and Davis [6]. However, Jungels, Raya and Hubaux’s scheme increase the robustness against packet losses since accusations are repeated periodically. The accusations are forwarded to the CA as soon as a connection to the CA is detected. An accusation based scheme is also suggested in [7].

In the certificate revocation list (CRL) method a Certificate Authority (CA) periodically updates a signed and time-stamped list of all revoked certificates. A major drawback is that with certificate lifetimes typically measured in years, even a small revocation rate may lead to long lists and do not scale very well. Therefore, CRLs are typically updated only weekly or biweekly [26]. Higher granularity is needed in order to be able to expel nodes from MANETs operation life of hours or days.

Morogan and Muftic [18] suggest the nodes of mobile ad hoc networks fetch CRLs when they are online on the Internet, or receive CRLs from nodes with fresher CRLs than their own.

Δ-CRLs are shorter and provide fresher information than CRLs as these lists only contain the certificates that have been revoked since last CRL update. If one or more nodes missed the last CRL, the complete CRL still needs to be distributed.

Eichler and Müller-Rathgeber [10] show that neither NOVOMODO (CRS) [17] nor Δ-CRLs are superior to the other in ad hoc networks.

Most of the information in the CRLs and Δ-CRLs will normally concern other nodes than those present in the specific MANET, and will never be used.

Common drawbacks of these schemes in ad hoc networks are the bandwidth consumption of accusations, CRLs and download from trusted entities during periods with connection to the fixed network. Our contribution is the SHARL scheme which provides flexible and efficient distribution of revocation information in ad hoc networks. The scheme utilizes the fixed network to maintain the full revocation list (RL). Only the subset of the RL relevant for a specific MANET is distributed into the ad hoc network – in the form of an ARL. In addition, the revocation lists (ARLs) are combined with the routers control messages, and thus contribute to bandwidth efficiency. This means, additional packet transmissions and extra message signature validation is avoided. Still, is the security requirement fulfilled when the central trusted entity and the routing messages have signed the ARLs. Other requirements for the SHARL scheme are robustness, simplicity and scalability.

- **Security**: The revocation information must be distributed in a manner that enables the recipient to verify its integrity, authenticity and freshness. The revocation information must reach the nodes in a timely manner.

- **Robustness**: The distribution of revocation information must be robust both to packet losses and nodes exhibiting Byzantine behavior. In operational scenarios such as emergency and rescue operations, availability is a number one concern. No false revocations should ever occur.

- **Simplicity**: Simplicity is an intuitive and overall design criterion. Computational complexity should be localized to the less constrained nodes. The decision to revoke a node may be made by an operator, but the distribution of revocation information should not involve human interaction.

- **Scalability**: The revocation scheme should scale well enough to handle the expected number of nodes, security domains, and revocations. The revocation information must be distributed in a bandwidth efficient manner. Redundant and irrelevant revocation information should be minimized.

The rest of this paper is organized as follows. The SHARL scheme is described in section II. Section III sketches implementation of the SHARL scheme with various routing protocols. The scheme is analyzed in section IV. Conclusions and application for the scheme are found in section VI and V.

II. THE SHARL SCHEME

A. Assumptions

An ARL (Ad hoc revocation list) contains revocation information concerning nodes in a specific MANET. The term revocation list (RL) is used to encompass both traditional certificate based public keys as well as identity-based schemes.

A central trusted entity is assumed in each security domain. This entity issues certificates or private keys, and is responsible for revocations. The keys are linked to IP addresses used by the routing protocol as identifiers, – either through certificates or by using the IDs as public keys. Each node may still use multiple and temporary identifiers. That is, only pre-defined nodes will expectedly be authorized to join protected ad hoc networks for emergency and rescue operations.

The general assumption that the IP addresses should be obtained as the node enters the network, may not apply. Home addresses of Mobile IP may be utilized. This is described in [12].
The MANET may include nodes from a single security domain or from multiple security domains, but not all nodes are currently included in MANETs. The central trusted entity defines a security domain which includes one or more MANET through gateway(s), see Figure 1. The central trusted entity issues a full RL on a regular basis. Full RLs are transferred to the nodes prior to MANET participation. The ARLs are distributed when MANET operation with the aid of trusted MANET gateways. In addition, the nodes must trust the MANET gateway to correctly report all nodes in MANET to the central trusted entity. The ARLs will be short and fit into a single routing protocol packet/message.

The gateways are assumed to be better protected and less resource constrained than ordinary MANET nodes. Some keys are specified for trusted gateways. The central trusted entity is assumed to possess computational and communicational resources large enough to handle the expected number of concurrent MANET instantiations. It is also assumed to be accessible from the trusted MANET gateways when needed. A revocation may be a result of detected malicious behavior, a report of a lost unit.

B. Protocol outline

1) The protocol between the central trusted entity and the trusted MANET gateway

The SHARL protocol is shown in Figure 2. The notation “A->B: MSG\_NAME, {MSG\_NAME}\_signA” means that ID A sends a message named MSG\_NAME to ID B, and {MSG\_NAME}\_signA denotes the results of applying A’s signature to data MSG. In the figure, A refers to the trusted gateway and B to the central trusted entity.

The protocol contains two mechanisms, mutual authentication which is provided by the first three steps in Figure 2, plus revocation provided by the two latest steps. The revocation lists are signed by the central trusted entity (B) and the trusted gateway (A) before the ARL is sent to the nodes in the ad hoc networks. The first three steps of the SHARL protocol is parallel to the three-pass mutual authentication mechanism specified in ITU-T Rec. X.509 [14].

The MANET gateway initiates the setup of an ARL with an SHARL initialization request (AREQ) message (step 1) in Figure 2. AREQ contains source ID, destination ID and a fresh generated sequence number (SeqA1). The central trusted entity responds with SHARL-initialization proceeds (APRO) message. The APRO contains source ID, destination ID, a fresh sequence number from the central trusted entity (SeqB1) and a receipt of the sequence number from the gateway (SeqA1). Messages where the signature check fails are discarded.

The MANET gateway proceeds with a Report & Refresh (RR) message which contains source ID, destination ID, the fresh incremented sequence number (SeqA2) and the receipt sequence number (SeqB1) from the trusted gateway. Additionally, RR message lists the IDs detected in the MANET. The central trusted entity registers the reported nodes and returns an ARL in step 4. The ARL lists the revoked IDs or revoked certificate serial numbers among the reported nodes. It may contain zero or more entries. The version number (RL no) is incremented only when new items are added to the list. In additional, the SHARL issuing (ARL) contains sequence numbers and ID’s.

After the ARL has been established, the SHARL protocol continues with repeating steps 3 and 4, see Figure 4. The uniqueness and freshness of the messages are evaluated with the aid of incremented sequence numbers SeqAi in RR and SeqBi in ARL messages. The periodic RR messages serve the dual purpose of reporting new nodes discovered (if any) and informing the central trusted entity of the continued existence of the MANET. An ARL is returned in response to each RR message. Reported IDs need not be repeated. If a RR message has not been received within a given period of time, the central trusted entity considers the MANET terminated. If continued service is demanded, and the gateway has not received an ARL in response to a given number of RRs, it reverts to step 1.

A MANET may have more than one gateway to the external network. The central trusted entity maintains a separate ARL for each gateway, no matter whether the gateways report the same set of MANET nodes or not. The MANET gateways run one instance of the protocol for each involved security domain (Figure 1.) and receive an ARL from each involved central trusted entity. When a node is reported in one or more MANETs, the central trusted entity considers the MANET terminated. If continued service is demanded, and the gateway has not received an ARL in response to a given number of RRs, it reverts to step 1.

© 2008 ACADEMY PUBLISHER
Protocol messages

\[ MSG_{AREQ} = \{AREQ, A, SeqA1, B\}, \]
\[ MSG_{APRO} = \{APRO, B, SeqB1, A, SeqA1\}, \]
\[ MSG_{RR} = \{RR, A, SeqA2, B, SeqB1, #IDs, IDs\}, \]
\[ MSG_{ARL} = \{ARL, B, SeqB2, A, SeqA2, RLno, #revoked, revoked IDs\}. \]

SHARL initialization messages (initial handshake)
1. A->B: SHARL INIT. REQUEST (AREQ): 
\[ MSG_{AREQ}, \{signA\} \]
2. B->A: SHARL INIT. PROCEED (APRO): 
\[ MSG_{APRO}, \{signB\} \]

SHARL maintenance messages (periodical)
3. A->B: REPORT & REFRESH (RR): 
\[ MSG_{RR}, \{signA\} \]
4. B->A: SHARL ISSUING (ARL): 
\[ MSG_{ARL}, \{signB\} \]

General message format (some fields may be empty):
Message type, Source ID, Source sequence number, Destination ID, Last received sequence number from destination, List version number, # IDs on list, List of IDs, Source’s signature.

(“#” = “The number of”)

Figure 2. The SHARL protocol between the trusted MANET Gateway (A) and the central trusted entity (B).

A->MANET nodes:
\[ \{A, Message sequence number, [Ordinary routing message body], ARL \} | signA \]

Figure 3. ARL distribution in the MANET.

2) The trusted MANET Gateway and the MANET nodes
The MANET gateways distribute the ARLs as a separate routing message/packet or appended to an existing flooded routing message type. The protocol is illustrated in Figure 3. The SHARL scheme assumes that the routing messages are protected by a cryptographic signature covering both the ARL as well as all other non-mutable fields of the routing message. The “ordinary routing message body” is only included if the ARL is appended to another routing message. Only non-empty ARLs are sent into the MANET. The latest non-empty ARL is flooded periodically. If multiple security domains are involved, more than one ARL may be included by the gateway.

The protocol between the central trusted entity, the gateway and the MANET nodes is outlined in the message sequence (MSC) diagram in Figure 4.

3) Message processing in the MANET nodes
The revocation information distributed with the routing protocol needs only be checked when the first ARL is received and when the RL number indicates a change in the list. Routing messages from revoked nodes are discarded.

III. THE SHARL SCHEME WITH VARIOUS ROUTING PROTOCOLS
To illustrate the usability of the scheme, we have described the possible integration with three different ad hoc routing protocols. We chose the protocols used as the basis for the standardization in the IETF Manet group.

OLSR: In the optimized link state routing protocol (OLSR) [2][4], all nodes maintain a view of the topology of the entire ad hoc network. Topology information, including gateway announcements, is distributed periodically with the aid of Multipoint Relay (MPR) nodes. Each node selects MPRs from its 1-hop neighbors in such a way that all 2-hop neighbors are covered by at least one MPR. Only nodes that are chosen as MPRs forward routing information. Each node is uniquely identified by its main address that is included in all messages.

OLSRv1[4] proposes that extensions to the protocol are implemented as new message types. OLSRv2 [2] adopts the generalized MANET packet and message formats specified in [3], and suggests extensions are implemented as new message types or type-length-value fields (TLVs) added to existing message types. For bandwidth efficiency, it is beneficial to include the ARL.
in existing routing messages. Additional packet transmissions and extra message signature validations are avoided.

OLSRv1 [4] specifies four message types: HELLO, Topology Control (TC), Multiple Interface Declaration (MID) and Host and Network Association (HNA). The HELLO messages are used for local link sensing, neighbor detection and MPR selection, and are not forwarded by the MPRs. The other message types are: TC messages convey topology information, and are only sent by MPR nodes. The gateway may not be chosen as MPR. Nodes with multiple OLSR addresses send MID messages to map these interface addresses to the main address. The gateway may not have multiple OLSR interfaces. As the revocation information is distributed through gateways, HNA messages announcing non-OLSR interfaces are a natural candidate for the inclusion of ARLs. OLSRv2 only specifies HELLO and TC messages. Gateway announcements are included as TLVs in TC messages. Hence, gateways emit TC messages, and ARLs can be added as TLVs to these.

The inclusion of ARLs as TLVs in OLSRv1 HNA messages is sketched in Figure 5. The SHARL scheme assumes that the routing messages are protected end-to-end by a message authentication TLV, e.g., using the scheme in [11]. Backward compatibility would require a new message type for ARLs. However, the inclusion of signature TLVs is also not backward compatible. According to the specifications in [4] signatures should also be distributed in separate messages. But, in [24] it is shown that end-to-end signatures in separate messages scale badly. And backward compatibility may not be important in operational scenarios such as emergency and rescue operations where only pre-defined nodes are allowed to join.

A potential problem is that only MPR selectors (nodes that have chosen this node as their MPR) are announced in the TC messages. Nodes that do not choose any MPRs could be accepted as symmetric neighbors, without having their existence exposed outside the scope of HELLO messages. However, in accordance with the OLSR specifications [4], the nodes can be set up to report all links. This will inhibit “hidden members”. Alternatively, the MPRs can report links to nodes that appears not to be included in any other TC messages.

**OSPF MANET:** OSPF MANET refers to the adaptation of the Open shortest path first (OSPF) [5] [19] routing protocol to ad hoc networks. Opposing OLSR, OSPF MANET provides reliable flooding. The proposed OSPF MANET solutions; **OSPF overlapping relays (OSPF-OR)** [1] and **OSPF MANET designated router (OSPF-MDR)** [21], differ in the way they optimize the flooding of routing information. OSPF-OR nodes choose overlapping relays (ORs) parallel to the MPRs in OLSR. Non-OR nodes act as backup ORs that retransmit the routing messages if the ordinary OR fails to do so. OSPF-MDR use **MANET designated routers** (MDRs) to flood routing information. The decision to become a MDR or a backup designated router (BMDR) is made by the nodes themselves. All routing messages are acknowledged.

The nodes are uniquely identified by their router ID included in each routing packet. All routers within an OSPF area have a consistent link-state database. The link-state database contains a collection of LSAs (link-state advertisements) that describes the OSPF routing domain. The topology information is disseminated through link state update (LSU) packets containing link-state advertisements (LSAs). Gateways to other areas (border area router) run different instance of the routing protocol for each area. Only summary information from one area is distributed into another.

We assume the MANET is one OSPF area. The area border routers announce their gateway capabilities through LSU packets containing inter-area-prefix LSAs and inter-area-router LSAs. We assume that the ARLs are included in LSU from trusted MANET area border routers. The other OSPF packet types; HELLO, database description (DD), link-state request, and link-state acknowledgement are not forwarded outside the 1-hop neighborhood.

The OSPF-OR and OSPF-MDR extensions to the OSPFv3 packet format is shown in Figure 6. MANET specific information is carried in a link local signaling (LLS) data block attached to HELLO and DD packets. OSPF-OR in addition specifies a new LSA type – link LSA that is used to distribute information about 2-hop neighbors. Each LLS data block may contain several TLVs. LLS-incapable routers will not consider extra data that follows after the packet. Thus, the attached LLS data
RREQ was received. The AODV specification unicasts a route reply (RREP) along the path that the intermediate nodes with a valid route to the destination (AODV) or the originator as well as the destination. The destination (or network. The RREQ carries the IP addresses of the LSAs could be modified hop by hop.) assumes the ARLs distributed in TLVs in a LLS data block attached to the LSU packets. The scope of the LLS thus becomes MANET-local rather than link-local. OSPF-OR [1] assumes LLS data blocks are appended to HELLO or DD packets used in the synchronization of the link-state databases of adjacent nodes. But LLS data blocks could also be attached to other packet types. We assume end-to-end protection of the routing information is implemented with signatures in TLVs in the LLS data block. It requires LSU packets are flooded as is. (OSPF assumes LSAs are flooded. The LSU encapsulating the LSAs could be modified hop by hop.)

Whereas OSPFv2[19] specifies authentication as an integral part of the routing protocol, OSPFv3 [5] relies on IPsec. OSPF-OR suggests the ability to connect to the MANET is controlled by layer 2 security mechanisms such as IEEE802.11i. The SHARL scheme can be used no matter which layer protects the routing messages. That is, at least as long as an asymmetric scheme is used and the revoked keys can be linked to IDs known to the routing protocol. IPsec and IEEE802.11i by default use symmetric keys. Unilateral authentication of ad hoc routing messages may imply a modification to the existing standards.

**AODV:** In the ad hoc on demand distance vector (AODV)[22] routing protocol, routes are discovered on demand by flooding a route request (RREQ) into the network. The RREQ carries the IP addresses of the originator as well as the destination. The destination (or intermediate nodes with a valid route to the destination) unicasts a route reply (RREP) along the path that the RREQ was received. The AODV specification [22] allows extensions in the form of type-length-value (TLVs) appended to RREQs and RREPs. We assume that all routing messages are integrity protected and authenticated by digital or identity-based signatures.

The gateways will normally not have a complete map of all nodes in the MANET. They can listen to the routing messages that are flooded in the network, and report to the central trusted entity as IDs are discovered. However, the destination will return a RREP along the path it received the RREQ. If the destination lies between the source and the gateway, the gateway may not receive any of the messages. The AODV expanding ring search, i.e., the flooding scope of RREQs is gradually increased until a route reply is received, makes it even less likely. Besides, intermediate nodes in a path will not be announced. Inclusion of the SHARL scheme demands a modification of the protocol; all nodes on an active path must periodically send a RREQ searching a gateway. The “D flag” must be set to avoid intermediate nodes with a valid route answers the request. The gateway checks the signature of the RREQ before the node is reported. If a node on an active path does not hear such RREQs originated from one of the precursors within a given period of time, the precursor is reported in a TLV appended to its next gateway RREQ or blacklisted (excluded).

The ARLs are added to RREQs sent by the gateway to a predefined revocation information address. All nodes processes and forwards the RREQ, but do not return any RREPs.

### IV. Analysis

#### A. Security evaluation

A Dolev-Yao threat model [9] is assumed, i.e. 1) cryptography is perfect: the adversary cannot produce a valid signature on other nodes’ behalf or decrypt a message that has been encrypted with a key it does not possess and 2) the ad hoc network is under full control of the adversary: it can eavesdrop on any message inserted, remove or modify messages, replay messages or forge source and destination addresses. Dolev Yao developed the first formalization of an intruder model and it is commonly used in many formal methods of security protocol analysis. We use a formal method to analyze and verify the authenticity and integrity of the protocol between the central trusted entity and the gateway.

1) **Formal method**

The correctness of the SHARL protocol is analyzed by using the formal method tool, Scyther [32]. Formal methods mean a formal description of the system behavior to determine whether a proof is correct or not according to the system security requirements [30]. The state of the art for automatic verification of security protocols using modern methods are Scyther [33] and AVISPA [34]. We have chosen Scyther, which is an effective formal method tool for verification of correctness of security protocols. The tool is based on two different techniques: a finite state model checker [35] and a backward symbolic state search technique [36].

The Scyther tool uses the concepts [32] roles, runs and agents to describe the behavior of the security protocol. The security protocol specification defines exchange of message between agents. This means, the gateway(s) and the central trusted entity are defined as agents in the SHARL specification. Each agent performs one or more roles. When the protocol execute, each role can be executed a number of times by multiple agents. The execution of a role is called a run. The roles are either initiator role or responder role in the protocol and each

---

*Figure 6. OSPF MANET packet extension*
role has send events and read events, shown in Figure 7. The events in the message sequence chart (MSC-diagram) correspond to the messages in the communication protocol in Figure 2. The Scyther tool checks the correctness of the security protocols by executing different runs of agents in each role and then verifies the synchronization/authenticity or agreement [31] of the protocol.

2) The security evaluation of the parameters in the protocol

The formal description of the protocol is idealized with focus on the necessary security parameters. The idealized SHARL protocol contains the parameters; sequence numbers (SeqA/SeqB) and the Destination ID’s (A and B). The rest of the parameters; AREQ, Source ID’s, APRO, RR, #IDs, IDs, ARL, RL no, #revoked and revoked IDs are not necessary for the mutual authentication of the protocol between the central trusted entity and the gateway.

Two simulations of SHARL protocol were conducted; the first included all parameters shown in Figure 2, while the second was based on the idealized version. We verified the same results from both simulations using Scyther; no attacks were related to authenticity or integrity. This means, to achieve the integrity or authenticity it requires that the Destination IDs and the sequence numbers have to be included in the protocol. The Source IDs are not necessary for the authenticity. This parameter will depend on the system behaviors and environments. This means, the Source IDs is optional for the SHARL protocol and it is used for easily finding the public key when messages are received. The rest of the parameters AREQ, APRO, RR, #IDs, IDs, ARL, RL no, #revoked and revoked IDs are necessary for the revocation mechanisms and have to be signed.

Further we analyzed the parameters; Destination IDs and sequence numbers, and evaluated theirs influence on the revocation mechanisms.

3) Sequence number evaluation

The sequence numbers in SHARL are related to the time variant parameter defined in ISO-9798-1 standard, Annex B [15]. To verify the importance of the sequence numbers, we modified the SHARL protocol. We repeat the sequence number (SeqA1) from message 2 into message 4 in Figure 2. The results from Scyther simulations showed a replay attack. This means, the sequence number can not be repeated or accepted more than once i.e. freshness. Additionally, the sequence numbers will be accepted according to some policy; 1) A message is rejected if the sequence numbers are repeated or not in sequence. 2) The sequence numbers shall not be reused during the lifetime of the signature keys. 3) The sequence number shall evaluate the uniqueness of the next messages in such a way that each message has to be linked to the preceding one. 4) The sequence number has to restart the counters when a RR message has not been received within a given period. 5) Each message has to be uniquely identifiable.

4) Identity evaluation

The sequence numbers are not enough to satisfy the uniqueness of the messages. It is also necessary to include the Destination IDs. BAN logic [29] was the first formal method which in 1989 verified a man in the middle attack on the X.509 protocol [14] can be avoided by including the destination ID’s in all three protocol steps. The three first steps of SHARL (see Figure 2.) are parallel to the X.509 protocol. The Steps 3 and 4 of the SHARL protocol belongs to the revocation mechanism.

We analyzed the importance of the Destination IDs for the revocation mechanism of the protocol. This was verified by removing the Destination ID in the last step of the SHARL protocol, step 4 in Figure 2. The results from the Scyther simulation detect replay and man in the middle attack. The attacks are explained in detail by using message sequence chart (MSC – diagram) shown in Figure 8.

The detection of the man in the middle attack starts in step 3 in the SHARL scheme. The message should go from A -> B, but Attacker (E) blocked and started a new session/communication to B.

Attacker (E) initiated a setup of SHARL with an AREQ message signed by herself, step 4 in Figure 8. The AREQ message contains Attackers’ new generated SeqC1 and IDs (source/destination). B responds APRO message. The APRO contains a fresh sequence number from B (SeqB1≠3) and a receipt of the sequence number from Attacker (E) (SeqC1). When Attacker (E) receives the APRO message from B, the attack is possible. Attacker proceeds with the RR message. The RR contains the sequence number (seqA2) from the trusted gateway (A) which central trusted entity B never has seen and a receipt of the sequence number from B (SeqB1≠3). In addition, RR contains the lists of IDs detected in the ad hoc network. This means, Attacker can forge IDs in the network, if the IDs are not unique in the security domain.
The attack occurs in the last step, the central trusted entity (B) responds with the ARL message to Attacker (E). The ARL message contains a fresh sequence number (SeqB2#3) and a receipt of the sequence number (SeqA2) from the gateway (A), which Attacker (E) replayed to the trusted central entity (B), see message number 7 in Figure 8. This means, the gateway knows that the signed ARL message is from the trusted entity, but the ARL message can contain forged IDs or certificate serial numbers among Attacker reported nodes.

The trusted gateway can avoid sending forged ARL message into the MANETs, because of the assumption of trusted gateways; Bs’ signature on the ARL message and the uniqueness of the IDs in the security domain. In addition, the ARL message contains the version number (RL no) which increments only when new items are added to the list, and that prevent the central trusted entity to send old ARL messages.

5) The security between the trusted MANET gateway to MANET nodes.

The ARL message in step 5, see Figure 3. includes the parameters (A, B, SeqB2, SeqA2, RLno, #revoked, revoked IDs). We have already verified that the parameters (A, B, SeqB2, SeqA2) are necessary for mutual authentication between the trusted entity and the trusted gateway, while the parameters (RLno, #revoked, revoked IDs) were necessary revocation information for the MANET nodes.

In some environments it may be possible to optimize the bandwidth consumption in the MANET by considering the ARL message in step 4. We assume that some keys are specified for trusted gateway, see section II. Additionally, the nodes has to know which nodes are trusted gateways, then the revocation information (RLno, #revoked, revoked IDs) could be a separate signed message $ARL_x \{RLno, #revoked, revoked IDs\}$. This means, the trusted gateway forwards the signed $ARL_x$ to the MANET nodes in step 5 in the SHARL protocol.

The central trusted entity’s signature of the $ARL_x$ in step 4 and the trusted gateway’s signature of the routing message in step 5 ensure the integrity of the revocation lists to the nodes in the MANETs.

B. Robustness and simplicity

The revocation scheme is simple and robust in the sense that there is no need to synchronize the revocation lists, even if not all ad hoc nodes have the latest full RL. If a revoked node is included in the network, it will appear in the next ARL, and be excluded. If a node is reported in more than one MANETs, the central trusted entity includes the node in all necessary ARLs. The MANETs receive an ARL from each involved central entity which has done the partition of the ARLs in the security domain. This means, there is no need for the gateways to synchronize their lists of nodes, and the central trusted entity needs not harmonize the various ARLs.

The scheme is robust to gateway failures in the sense that ARLs are deleted automatically if the central trusted entity has not receive any RRs within a given timeout period. The scheme is robust to packet losses. Non-empty ARLs are repeated in the periodical routing messages from the gateways. Bandwidth consumption is optimized as the ARLs only include information concerning the nodes in the specific MANET. Also, most of the SHARL administration is off-loaded to gateways and central trusted entities that are expected to be less energy-constrained than the battery powered ad hoc nodes.

No revocation information will be distributed unless a trusted gateway with access to the fixed net exists. A remedy could be to empower more protected and trusted ad hoc nodes to deny access; possibly implemented by a threshold scheme [8] (a threshold number of trusted nodes must co-operate to exclude a node). But it also adds complexity and increases bandwidth cost. He sends a message.

C. Scalability

Scalability is related to performance and timeliness, and depends on the number of the nodes and the number of revocation. The number of revocations in a specific MANET will depend on the size of the MANET and the lifetime of the network.

The performance of the SHARL scheme is represented by the central trusted entity’s processing load, MANET(s) gateway’s processing load, gateway to nodes communication overhead and finally nodes’ processing load. The load is critical from the trusted gateway(s) to

Figure 8. MSC for replay and man in the middle attack
the nodes because of bandwidth in MANET. The load is determined from the overhead between the trusted gateways and the central trusted entity. The overhead depends on the RR frequency, which can be scaled by the gateways. The sizes of the messages are determined by the number of nodes in the MANET and the signatures and message header information inserted by the gateway and the central trusted entity. The signatures will expectedly contribute most. Redundant revocation information is reduced as origination of ARL messages is limited to trusted MANET gateways, and only non-empty ARLs are sent into the network.

The SHARL scheme is here compared with CRLs and Δ-CRLs distributed through the gateways rather than the state-of-the-art accusation-based and CRL-exchange methods surveyed in section I. We consider CRLs and Δ-CRLs to be more likely alternatives for our operational scenario. Both CRLs and delta-CRLs have a much higher load and delay from the trusted gateways to nodes in MANET. This is because that all revocation information is sent to all MANETs which belong to the trusted central entity. The ARLs of the SHARL scheme contain only the subset of the RL that is relevant for the nodes in a specific MANET. The system application, environment and requirements are important for the chosen revocation scheme. The SHARL scheme is designed for revocation of keys used in communication networks or where not all nodes take part in the networks at all times.

Keys of central trusted entities are normally longer than those of ordinary nodes. The signature verification cost increases accordingly. This is optimized in that the MANET nodes only have to verify the ARL signature when a new ARL is flooded into the network. The number of changes will usually be much lower than the number of nodes in the network.

The SHARL scheme is more optimize for timeliness than CRLs or delta CRLs. The timeliness depends on the update period. Delta CRL can have more frequently updates than the CRLs. Δ-CRLs are shorter and provide fresher information. These only list certificates that have been revoked since last CRL update. In worst case the CRL can be as old as one update period. For delta CRL, the worst case is for newly registered nodes which do not get all revocation information, only the revocation related to the latest update period. Moreover, CRLs and Δ-CRLs normally list revocations concerning the entire security domain and not only the subset of nodes that takes part in a specific MANET. This represents a waste of bandwidth.

The SHARL scheme can offer more frequently updates than CRL and delta CRL. The SHARL scheme does not send empty ARLs to MANET. In addition SHARL is scalable because the number of revocations in the ARLs is for a specific MANET and not for the whole security domain. Furthermore, the cost and bandwidth efficiency contribute to the scalability.

V. APPLICATION

The system application, environment and requirements are important for the chosen revocation scheme. The SHARL scheme is designed for revocation of keys used to protect the ad hoc network service, and the ARLs are distributed with the routing messages in the ad hoc networks. An ad hoc network has strong requirement regarding bandwidth consumption. The SHARL protocol between gateway and the trusted entity is efficient regarding bandwidth consumption, as an ARL contains revocation information concerning nodes in a specific MANET. If the security domain contains only one MANET and all nodes in the security domain participates in the MANET, the ARL will be equal to a CRL. This means, the SHARL is optimized for bandwidth consumption and decentralized systems where the security domains contain more than one communication networks or where not all nodes takes part in the networks at all times.

VI. CONCLUSION

In the SHARL scheme, only revocation information that explicitly concerns the nodes in a specific MANET is disseminated into the ad hoc network. The overhead depends on the number of nodes in the ad hoc network rather than the total number of nodes in the involved security domain(s). This makes the SHARL scheme scale well.

The scheme requires that trusted MANET gateways can detect which nodes are in the network. This comes intrinsically with proactive routing protocols. We also described the implementation of the SHARL scheme with reactive routing protocols. Additionally, we verified the correctness of the SHARL scheme by the formal method tool Scyther. The protocol was proved to be correct. The parameter, source ID, was found not to be strictly required for the correctness of the protocol between the central trusted entity and the gateway and is optional in SHARL scheme (step 1-4). Another protocol optimizing is that the revocation list (ARL) in step 5 only contains (R,no, revoked, revoked IDs). This contributes to the efficiency of the bandwidth consumption in the MANETs.

When a node is reported in one or more MANETs, the central trusted entity includes the node in all necessary ARLs. The MANETs receive an ARL from each involved central entity which has done the partition of the ARLs in the security domain.

The SHARL scheme provides an efficient distribution of the revocation lists, because it utilizes the fixed network to maintain the full revocation list and distributes only the part of the list, ARLs. Further, the distributions of ARLs are included in routing messages. This means, additional packet transmissions and extra message signature validation is avoided and thus contribute to bandwidth efficiency in MANETs.

ACKNOWLEDGEMENT

This work was supported in part by grant from Department of Telematic and Q2S at Norwegian University in Trondheim, the Research Council of Norway, Microsoft in Norway, Kongsberg Defence & Aerospace and Ministry of Government Administration and Reform.
REFERENCES


[34] AVISPA. http://www.avispa-project.org/. The link was valid Oct. 2007.


Mona Holsve Ofigsbø received the Cand. Scient. degree in cybernetics from the University of Oslo, Norway 1993. She is a PhD candidate in the department of Telematics at Norwegian University of Science and Technology in Trondheim, Norway.

She has worked with packet radio networks and currently interested in PKI.

Anne Marie Hegland received her M.Sc. degree in electronics from the Norwegian University of Science and Technology in Trondheim, Norway in 1997, and a PhD in informatics from the University of Oslo, Oslo Norway in 2007. She has worked R&D within security and crypto equipment since she joined the Kongsberg Group in 1987. She is currently a Senior Systems Engineer at the Security and Concept Development Department of Kongsberg Defense & Aerospace, Billingsstad, Norway.
Pål Spilling obtained his cand. real. degree in physics from Oslo University in 1963. In January 1964 he started on a PhD-program at University of Utrecht the Netherlands, and finished his degree in summer 1968 in experimental low-energy neutron physics. Subsequently he joined the nuclear physics group at the Technical University in Eindhoven the Netherlands. In January 1972 Spilling started to work for the Norwegian Defense Research Establishment (FFI) at Kjeller, and from end 1974 he got involved with the ARPA-funded research program in packet switching and internet technology, under the leadership of Yngvar Lundh. He was in 1979/80 visiting scientist with SRI International in Menlo Park California, where he worked on the Packet Radio program. Spilling left FFI in August 1982 to join the Research Department of the Norwegian Telecommunications Administration (NTA-RD), also at Kjeller. Subsequently he established the first internet outside USA, interconnected with the US internet. At NTA-RD Spilling worked with communications security and the combination of internet technology and fiber-optical transmission network. In 1993 Spilling became professor at Department of informatics, Oslo University and University Graduate Center at Kjeller. He is now a professor emeritus.

Oyvind Kure is a professor at the center for Quantifiable Quality of Service in Communication Systems and in the department of Telematics, both at Norwegian University of Science and Technology, Trondheim, Norway. He got his PhD from University of California, Berkeley in 1988. His current research interest is various aspects of QoS.

Leif Nilsen received the Cand. real. degree in mathematics from the University of Oslo in 1977. He is presently working as expert at Thales Norway and as associate Professor at the University Graduate Center, UNIK. He has been doing research, development and lecturing in cryptography and information security since 1988 and has participated in international standardization in this area since 1990, including ISO/IEC JTC1 SC27 and ETSI SAGE. He has background from teaching in mathematics, physics and computer science and is author of several textbooks. He is Chairman for Program Committee for IKT-SoS under the Norwegian Research Council and was Chairman of Eurocrypt’93.

Mr. Nilsen is a member of the International Association for Cryptographic Research.