Trust Agreement in Wireless Mesh Networks

Andreas Noack

Trust Agreement in Wireless Mesh Networks

Andreas Noack

Horst Görtz Institute for IT-Security
Ruhr University Bochum

Abstract. Establishing a trust relationship in decentralized wireless mesh networks (WMN) is an open question to date. In MANETs and cable bound meshed networks (like the Internet) there are a lot of proposals and solutions for trust establishment and for authentication.
In this paper we examine those existing solutions and analyze them for their applicability to wireless mesh networks.
We investigate the special demands of WMN, show the differences to existing network types and finally propose a trust agreement scheme that is particularly adapted to WMN.

Keywords: Wireless Mesh Networks, Trust Agreement, Reputation, Authentication, Authorization, Web of Trust.

1 Introduction

Imagine a group of wireless users in a city. These users are interconnected and some of them provide services like internet access or even an email service. Usually, the provider of a service does not want to offer his service to the whole world but only to a limited group of trusted users. On the other side there are users who only want to rely on trustful services, since no customer would like to use an email provider who eavesdrops on all his emails. The demand for a trust management system emerges.

Identification or at least the recognition of other users is an important issue for trust relations, because one can only have trust relations to users that you are able to authenticate. Authentication has been discussed widely for the classical internet and mobile ad-hoc networks (MANETs) [4][5]. But as far as we know, there is no feasible solution for authentication, recognition nor for trust establishment of nodes in Wireless Mesh Networks (WMN), which differ in several points from MANETs. WMN consist of static nodes, which have no computational nor battery power constraints and are able to do WiFi typical throughputs (11M, 54M, 300M) between neighboring nodes.

Wireless mesh networks are the "missing link" between the classical internet and mobile ad-hoc networks. Nodes in a MANET are mobile, whereas nodes on the internet are completely stationary. Wireless mesh networks are located in between, as the backbone of a WMN is mainly stationary. Nevertheless the availability and reachability of nodes is not nearly as good as on the internet due

to wireless communication. Wireless interference has a big influence on the links and plays therefore a big role in wireless mesh networks, as it does in MANETs.

In practice, wireless mesh networks can be found in community networks like SeattleWireless [2] or MIT Roofnet [1], industry projects (e.g. metalworking industry) and even military projects. Most of these networks grow irregularly while being bound to a specific environment, thus we cannot assume a clear network structure in most cases. We therefore assume that a WMN is a decentralized network without a central node that is reachable all the time (due to the limited reachability in WMN).

In this paper, we propose a protocol scheme for trust establishment that is optimized for wireless mesh networks. There are several solutions in the MANET and peer-to-peer world that support reaching the goal, e.g. offline CAs with hierarchical trust structure, virtual or distributed CAs (e.g. with threshold cryptography), ID-based key agreement, reputation management systems, the web of trust technique and many more [12][13][10][9].

We discuss the existing approaches regarding their feasibility for wireless mesh networks and conclude with a new trust agreement scheme for wireless mesh networks that combines and extends the most feasible ideas.

2 Differences to MANETs

Our contribution is particularly directed to wireless mesh networks. In order to delimitate our results from MANET solutions, we outline the essential differences between MA-NETs and WMN.

Mobile ad-hoc networks consist of a loose aggregation of mobile nodes. This means, the wireless link quality and also the link duration is fluctuating very randomly. When a node's link disconnects or a new link is established, the routing topology changes. Therefore it is not assured that each node can be reached at any time. Wireless mesh networks also rely on wireless links, but their nodes are more or less static in their position. Therefore the link duration is notably longer, although the link quality may fluctuate due to wireless interference. The frequency of topology changes in WMN is more similar to the internet than to MANETs and thus the proposed authentication mechanisms can be optimized for longer living connections.

Moreover most MANETs (e.g. sensor networks, VANETs and many more) are based on simple hardware components, so that there is usually limited computation power and sometimes even a limited energy supply, i.e. we have battery powered devices. These limitations are not present for WMN, leading to the capability of performing longer and more complex computations.

Due to the minor mobility of WMN nodes and no power limitations, WMN nodes can be equipped with more than one radio interface, using different wireless channels. This leads to far higher bandwidth as can be provided by MANETs, since half-duplex effects can be avoided and wireless interference is reduced.

2.1 Technical Design Goals

We design a trust establishment scheme that is particularly adapted to wireless mesh networks. For optimal compliance with this kind of network, the design has to be influenced by the advantages and restrictions that are provided by WMN.

The desired scheme should make use of local broadcasts, since they are cheap in wireless networks due to the wireless propagation of the signals.

In contrast to cable bound networks, we have higher packet loss rates in wireless networks because of wireless interference, range constraints and thereof resulting route changes. Usually, the occurence of packet loss in wireless networks is not uniformly distributed which results in phases with a good link and phases where nearly no packet passes through the network. It is sensible to minimize the number of messages to compensate the packet loss effect by having shorter sending periods. But if there is a connection, we are normally able to retrieve a high throughput in WMN (several radios, several channels, more transmit power than in MANETs). A good choice for the packet size is therefore near the maximum transfer unit (MTU), for the reason that the currently given throughput should not be limited by protocol overhead. To prevent packet fragmentation which would introduce a higher dropping probability (for the aggregated packet) and the need for a more complex retransmission mechanism, the packet size should obviously not exceed the MTU.

Furthermore the design has to consider a decentralized structure where no particular node can be a single point of failure, since wireless links (meshed wireless links are even worse) are not reliable in comparison to wired links.

As distinguished from MANETs, we have a much greater computation power and memory, while having no power constraints. This allows us to use complex mathematics like asymmetric cryptography, also elliptic curve based cryptography is imaginable. Trivial parts like an integrated clock or persistent memory, which can be absent in low cost devices, are furthermore assumed to be available in WMN devices.

Finally there is a further important point that will influence the design of the trust establishment scheme: The differentiation between important and and less important nodes. Important nodes are nodes that forward a lot of userdata, e.g. nodes that are located in the middle of the network or right before an internet uplink. These nodes obviously need a higher trust level than less important nodes that are e.g. located at the border of the network and do not forward any foreign data.

3 Related Work

On the way to our goal there are some issues to solve, e.g. there is the need for recognizing other users, since it is not possible to establish trust relations with a group of users that cannot be distinguished. This can on the one hand be handled by recognition techniques (e.g. a self signed public key pair) and on the other hand by common authentication schemes. In this section we give an overview

about existing approaches for authentication from neighbouring research fields like the internet communication, MANETs and peer-to-peer networks.

- An *authentication server*, i.e. an AAA server or online certification authority (CA), authenticates clients to a wireless network. Cheikhrouhou et al. [3] and Lin et al. [8] proposed schemes that realize authentication between clients and authenticators (i.e. border gateways, access points). Both proposed schemes need an online Trusted Third Party (TTP) in the background for authenticating clients and authenticators. These schemes do not provide mutual authentication between the clients.
- An *offline certification authority* (CA) issues public key certificates for each user. Each user is then able to verify public key certificates from other users by verifying the certification chain up to the CA. This idea is widely spread on the internet and in the MANET world [12][13][7]. The CA can either be inactive or offline as long as no user joins or leaves the group. If a new user wants to join, a certificate must be issued. If a user leaves the group, a certificate revocation is required to preserve the consistency of the authentication process.
- A *distributed* or *virtual CA* issues public key certificates for each user, e.g. with the techniques from threshold cryptography [7]. A group of $k + 1$ randomly chosen CAs (or users) cooperates issuing or revocating a certificate for a certain user. Thus, revocation is possible without a particular TTP. Since for each new certificate or revocation a group of users (virtual/distributed CA) must cooperate, the solution is quite complex (in comparison with other solutions) and the deployed network protocol may need several rounds to complete. One proposal is given by Noack et al. [10].
- *Symmetric keys* for each pair of users. Each user shares a pairwise symmetric key with each other user of the network, leading to a large number of keys (exponential in the number of users). Certificate revocation lists or similar approaches are not needed, because single keys can be invalidated easily. Consider that when a new user joins or an active user leaves, all other users have to perform one key operation.
- *ID-based private keys* issued by an on demand CA. An on demand CA issues a private key (matching to the user's public key) for each new user. The special point is that everyone can compute the public keys of all users by using a common public value and the user's ID. Since everyone can compute the public keys and does not have to obtain them from a certain source, revocation is a challenging task. Zhang et al. proposed an ID-based authentication and billing scheme [14].
- *Self computed public key pairs* (e.g. self signed certificates) allow users to be cryptographically recognized. This idea can be extended with *trust agreement schemes*, like the web of trust technique, to add authentication due to transitive trust relations. However, for initial trust relationships there is the need for a trusted channel, i.e. a phone call to compare the public key fingerprints of each other. In completely autonomous networks without user interaction the trusted channel phase can be replaced by a multifactor

authentication (i.e. public key certificate, MAC address, neighbourhood, behavior fingerprinting, cryptographic token, etc.).
The revocation of trust values can be handled by the trust agreement mechanism itself, similar to a certificate revocation.

- *Reputation management* schemes are used to classify the behavior or the grade of authentication of particular users. The global reputation of a particular user is calculated by the aggregation of votes by other users. Nithyanand et al. proposed a privacy preserving reputation management scheme for peer-to-peer networks [9]. Kamvar et al. introduce the EigenTrust reputation management algorithm to peer-to-peer networks, which helps to eliminate inauthentic files in file-sharing networks [6]. On the internet, reputation systems are also very common (i.e. ebay.com, amazon.com, etc.) [11], whereby the idea that is behind reputation management still remains untouched.

Wireless mesh networks have a decentralized structure that enables an autoconfiguration and self-healing ability. To preserve these abilities, a trust agreement or an authentication scheme (as a part of it) should not depend on a single party leading to a single point of failure.
Keeping this in mind, three techniques remain suitable for wireless mesh networks:

(1) a virtual or distributed CA that issues public key certificates,
(2) the use of self signed public key certificates with trust agreement mechanisms as trust anchor and
(3) a decentralized reputation management scheme.

However, virtual/distributed CAs need at least $k+1$ cooperating users to perform operations, whereas trust agreement and reputation management schemes do not have such restrictions. Therefore a mixture of trust agreement and reputation management turns out to be appropriate for a wireless network that does not provide full reachability of the nodes at any time.

4 Trust Agreement

Trust between users is an important point in wireless mesh networks. Only if a trust relationship is given, confidentiality and integrity make sense. Informally spoken, trust has a recognition (or authentication) part and a valuing part. Recognition is needed for being able to distinguish a user from other users which is obviously very important for trust relationships. The latter part of trust is a valuing part, used to express how trusted a user is.

Definition 1. *Trust Agreement means the establishment of trust relationships between all users of a group, whereby a trust relationship is the recognition of a particular user and a value that describes, how trusted this user is.*

In this section, we introduce a trust agreement technique to establish trust relations in WMN. To create a common trust base, we use direct as well as transitive trust relations between particular peers and combine them to a common view. The final goal is to create a trust network, in which each of the mesh networks' peers are included and each peer has a trust opinion of all other peers.

We proceed with a distinction of Trust Agreement and Web of Trust, which are important to not confuse with each other. Later on we present our idea of abstract trust requirements, define trust in WMN and propose a technical solution for creating trust in a network. All the steps are combined to a full trust agreement scheme in section 5.

4.1 Trust Agreement vs. Web of Trust

Trust agreement and web of trust are completely different concepts for dealing with trust in a network. The most important difference between trust agreement and web of trust is the trust view on the network. With trust agreement, one common trust view for all users is computed, whereas each user in a Web of Trust has its own trust view on the network.

Both solutions have advantages: Web of Trust is closer to reality, since it is natural that trust to a certain person is different for two independent persons. Usually your wife has a higher trust in you than a randomly chosen person from the street. Trust agreement, however, creates one global trust value for each user. Though this is not a realistic circumstance, trust agreement has some crucial advantages over web of trust. Firstly, if trust opinions on one user differ very much, the relevance of these opinions decreases for all other participants, since they probably do not have the ability to choose the right opinion. This is a general problem of trust, which is adapted by the web of trust technique and which can only be handled with a complete (transitive) trust view or a sensible average function. Secondly, most users do not know every other user of the network from the beginning. An initial trust value has to be assumed for unknown users. Trust agreement solves this by providing a sensible initial trust value for each user that was computed in a collective manner. After becoming an active participant of the network, you are able to influence the agreed trust value of a certain user with own trust impressions. Thirdly, if the system is operated autonomously, we require a simple system for authentication or recognition. Web of trust is problematic, since it does not provide a single trust view on the network that would be needed to create a robust network. Different trust opinions on one user can lead to divergency problems, e.g. a fully authenticated path for Alice may not be authenticated for Bob.

Therefore the best tradeoff is providing a trust agreement scheme that provides a globally agreed trust value for each user. This is what we are proposing in the following.

4.2 Abstract Trust Requirements

Wireless mesh nodes have different trust requirements concerning their position in the mesh network graph. We are beginning with the assignment of abstract trust requirement levels to different positions in the WMN. The idea of differentiating several positions in the network is similar to the different roles of autonomous systems in internet routing (stub, multi-homed and transit AS).

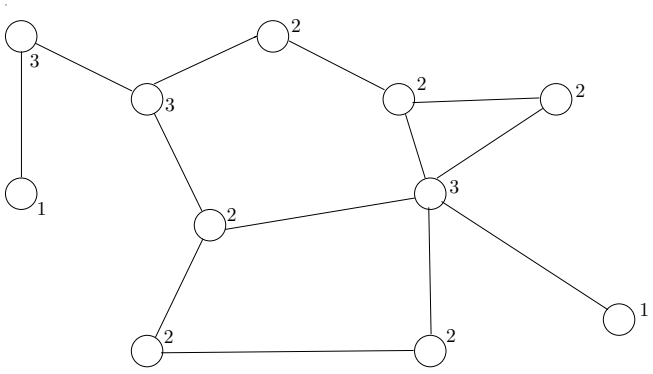

Fig. 1. Abstract trust requirement levels in a WMN

We assign numbers between "1" and "3", whereby a higher number means a higher trust requirement. Nodes with only one edge are mesh participants, who do not forward any data from other nodes. Since their responsibility and trustworthiness is quite low, they just need a low trust requirement (indicated by "1" in figure 1).

Nodes with at least two edges have a higher trust requirement, because they are forwarding data from other nodes. We distinguish between nodes, for which an alternative path exists and nodes, that cannot be avoided by at least one other node. So we introduce two trust requirements: "2" for routing nodes that can be circumvented and "3" for routing nodes without an alternative path.

Trust requirements are allocated on behalf of the amount of foreign data that passes a node. We think that it is very important to care for the honest handling of foreign data, which is transmitted in cleartext in the most practical wireless mesh networks to date. Thus we only refer to security and exclude availability and performance in this paper. Of course a reduced availability of a node will have impact on its trust value, but only because of a shorter availability time.

Additionally to the given trust requirements we provide an extended version in Appendix A.1, introducing a more practical and precise classification.

4.3 Definition of Trust in Wireless Mesh Networks

There are two different understandings of trust in wireless mesh networks: local and global. Local trust (later used as trust assignment) is the reputation mean-

ing, one has towards a particular user. Global trust is the final trust level, a user gains after aggregating all local trust values.

In this section, we define the composition of trust in general. By our definition, trust in wireless mesh networks consists of two parts:

Definition 2. *Trust in wireless mesh networks is determined by a trust tuple* (α, θ). $\alpha \in \boldsymbol{N}^+$ *represents the authentication and* $\theta \in \boldsymbol{R}^+$ *the grade of authorization.*

The first part is the recognition or authentication part which is necessary to distinguish nodes from each other. Recognition means that every node has a distinct cryptographic attribute (e.g. a self signed certificate) that proves his binding to a self chosen identity. Authentication extends this by creating a cryptographic binding to an approved identity. Actually, authentication and recognition are binary decisions, because there are always only two possibilites: you have identified a user or you have not. After all, the authentication value α is determined by the addition of all binary authentication results. However, the value of α (if greater than one) is not the determining part of the trust level, it just represents the number of nodes who authenticated a certain node.

The second part of trust is a valuing component, namely how trusted a user is. We call this part authorization value, since it will be used to authorize users to become part of the network. Later on, the authorization value can also be used for choosing the best (most trustful) route for a packet through the network, if our scheme is combined with a source routing algorithm. Authorization is expressed by the real value θ.

4.4 Creating the Trust Network

Trust agreement bases on a simple reputation assignment and signing mechanism with the following basic idea:

If a particular user U_i trusts another user U_j with $i \neq j$ (local trust), U_i creates a trust assignment $T_{ij} = (\alpha_{ij}, \theta_{ij}, \mathrm{VD})$ and broadcasts this assignment together with a corresponding signature σ_i (signed with U_i's private key SK_i).

- $\alpha_{ij} \in \{0, 1\}$ represents the recognition/authentication from U_j towards U_i as a binary value ($1 \rightarrow$ trusted, $0 \rightarrow$ untrusted). However, an authentication is always a binary decision, since there are only two possibilities: U_i knows U_j or not. Revocation can also be handled with α_{ij}; its value has to be 0 in that case.

  In autonomous networks, recognition of other users is usually used instead of a full authentication. In this case, α_{ij} is 1 if the user U_i has made any experiences with user U_j, else α_{ij} is 0. If a full authentication scheme is used, U_i has to fetch an authentication evidence of U_j. This can be done by a personal meeting of both users, a comparison of the public key fingerprints by phone, a multifactor authentication or via many other ways.

- $\theta_{ij} \in \{0 \dots \theta_i\}$ is the grade of authorization given by the user U_i to the user U_j. The upper bound of the issued authorization value is fixed by the user U_i's own (global) authorization value.
- VD (Validity Date) represents the date, when the given trust assignment expires. Therefore, trust assignments have to be refreshed regularly. A trust assignment with a posterior Validity Date replaces previous ones.

Definition 3. *A valid trust assignment (local trust) for user U_j issued by U_i consists of a vector $T_{ij} = (\alpha_{ij}, \theta_{ij}, VD)$ and a signature σ_i over this vector T_{ij}. The signature σ_i is computed with the secret key SK_i of U_i.*
Furthermore the trust assignment must have the following properties:

1. *The validity date VD must not be expired.*
2. *The authentication value α_{ij} must be 1 (if no revocation is intended).*
3. *If the issued authorization value θ_{ij} is intended to increase the authorization value of U_j: The issuer U_i's authorization value θ_i is bigger or equal than the receiver's θ_j plus the trust assignment's θ_{ij}. ($\theta_i \geq \theta_j + \theta_{ij}$)*
4. *If there is a trust assignment with $\alpha_{ij} = 0$, all trust assignments T_{kj} from U_k with $(\theta_k < \theta_i) \wedge (VD_{kj} < VD_{ij})$ are invalid.*

A trust assignment T_{ij} with an authentication value $\alpha_{ij} = 0$ is called revocation assignment. If a revocation assignment T_{ij} was issued to U_j, all trust assignments T_{kj} from U_k with lower authorization levels ($\theta_k < \theta_i$) *and* shorter validity dates ($\mathrm{VD}_k < \mathrm{VD}_i$) become invalid.

The global trust value of a particular user U_j is computed from all trust assignments (local trust) intended to him. A valid trust assignment contains a valid (not expired) VD and is signed from a user with a higher trust level, to prevent fraud. All valid trust assignment tuples are summed up componentwise, whereby each single authorization value θ_{ij} is multiplied with a coefficient ω before.

The coefficient ω is necessary in order to prevent a user U_i from transfering his complete trust to another user U_j, thus creating a more or equally trusted user than himself. ω is defined as $\frac{1}{s}$, whereby s equals the average number of ascertained trust assignments in the whole wireless mesh network.

Definition 4. *A user U_j's global trust value is computed as:*

$$(\alpha_j, \theta_j) := \Big(\sum_{\forall i: U_i \in S} \alpha_{ij}, \quad \sum_{\forall i: U_i \in S} \omega \cdot \theta_{ij} \Big)$$

whereby S is the set of users U_i who issued valid trust assignments.

Each wireless mesh network has a founder $\mathcal{F}$, who plays a distinguished role in the trust agreement scheme. The founder $\mathcal{F}$ has the highest authorization level $\theta_{\mathcal{F}}$ of the network and due to the design of our scheme, no one is able

to reach that level if $\mathcal{F}$ does not transfer his trust level directly. If the founder $\mathcal{F}$ leaves the network, the user with the highest trust level becomes the new founder. Trust assignments from $\mathcal{F}$ are summed up directly, without applying ω, to allow the network to grow faster.

Only summing up the particular trust assignments is the simplest and also the most obvious approach. Actually this might not be the best solution, so we give another (more complex) approach in Appendix A.2.

5 Trust Agreement Scheme

In this section, we define a full trust agreement scheme for wireless mesh networks in two steps: a startup phase to create a trust network from scratch and a subsequent phase for normal operation. We make use of the trust agreement technique introduced in the previous section and combine this with trust requirements for particular node positions in wireless mesh networks.

5.1 Startup

Each wireless mesh network is initiated by a founder node $\mathcal{F}$ resp. $U_{\mathcal{F}}$. All nodes U_i that are directly connected to $\mathcal{F}$ (not yet providing connectivity for other nodes) need a trust level of "1" according to the trust requirements from section 4.2.

Then, if an authentication scheme is used, $U_{\mathcal{F}}$ interacts with his neighbor nodes U_i, determining their identity e.g. with a multifactor authentication method. An example for a multifactor authentication may be the verification of: public key fingerprint + MAC/IP address + position in the network + hardware hash. If a recognition scheme is deployed, $U_{\mathcal{F}}$ only requests the identifying attributes (including a proof of possession) of his neighbor nodes U_i.

$U_{\mathcal{F}}$ issues trust assignments $T_{\mathcal{F}i} = (\alpha_{\mathcal{F}i}, \theta_{\mathcal{F}i}, \mathrm{VD})$ and a signature $\sigma_{\mathcal{F}}$ for each, whereby $\alpha_{\mathcal{F}i}$ is 1, $\theta_{\mathcal{F}i}$ is at least 1.0 (depending on the designated trust requirement for the node) and VD a date in the future.

5.2 Normal Operation

From now on, our trust agreement scheme is able to work decentralized, that means an operation without the founder. The trust agreement scheme is operating according to the following conditions:

(1) **IF** Authorization value θ_i at date $D_{\text{near future}} <$ trust requirement
THEN
Request trust assignments T_{ji} from surrounding nodes U_j.

(2) **IF** Authorization value θ_j of neighbor $U_j <$ trust requirement
THEN
Exclude U_j from routing.
Do not join network, if U_j provides the only connectivity.

(3) **IF** U_j behaves dishonestly, i.e. dropping or manipulating packets
THEN
Reduce assigned trust to U_j by sending a new T_{ij} with lower θ_{ij}.
(4) **IF** U_j behaves trustworthy for a time period $P_{\text{threshold}}$
THEN
Raise assigned trust to U_j by sending a new T_{ij} with higher θ_{ij}.
(5) **IF** Revocation assignment T_{ij} was issued to U_j
THEN
Trust assignments T_{kj} from U_k with $(\theta_k < \theta_i) \wedge (VD_{kj} < VD_{ij})$ have to be renewed.

Trust assignments T_{ij} are broadcasted through the whole network, enabling all nodes to compute a complete trust view over the mesh network. To make the network more robust, each node broadcasts his own trust value at regular intervals: $H_i := (\alpha_i, \theta_i, \text{VD})$ and a corresponding signature σ_i.

If a trust assignment T_{ji} (intended for U_i) does not reach all hosts, the provided H_i value by U_i will differ from the computed trust value on these (non reached) hosts. In this case, all trust assignments intended for U_i can be requested directly from U_i, who saves them locally.

Both time values $D_{\text{near future}}$ and $P_{\text{threshold}}$ are to be chosen in respect to the practical scenario and the security requirements.

6 Security Considerations

We outline the security of the presented scheme with an informal security proof. At first we give an overview about possible attacks on our scheme, followed by how our scheme is able to resist those attacks. Consider an adversary $\mathcal{A}$ as a probabilistic Turing machine, who has control over all communication channels.

(1) **Trust incrementation.** An adversary gains a higher authorization level by spoofing trust assignments (adressed to him).
(2) **Mutual trust incrementation.** n adversaries increase their authorization levels in a mutual way to gain a higher impact on the mesh network.
(3) **Malicious behavior.** An inside adversary revocates randomly or distributes bad trust assignments to trustful nodes.
(4) **Revocation circumvention.** When an adversary is revocated, he blocks the revocation messages by trustful nodes to stay alive in the mesh network.
(5) **Adding virtual aversaries.** One or a group of adversaries add new virtual adversaries, simulating their whole communication, to infiltrate the network.
(6) **Denial of service.** An adversary exhausts the node's computation power by forcing them to do diffcult and/or multiple computations like signature creation or signature verification.

For resisting the above mentioned attacks, our scheme provides several security mechanisms. In the following, we describe these counter-measures.

(1) **Trust incrementation.** A trust assignment $T_{i\mathcal{A}}$ needs a valid signature σ_i to become valid. Since we can assume that an computational bounded adversary $\mathcal{A}$ is not able to forge a digital signature from an uncompromised user U_i, we conclude that this attack cannot be successful.

(2) **Mutual trust incrementation.** Due to definition 3 (property 3), the issuer's authorization level is always greater or equal than the reveiver's authorization level. We follow that the highest authorization level within a group of adversaries cannot be increased without interaction of external nodes (i.e. trustful users).
Consider k adversaries and $\theta_{\max}$, the authorization level of the most trusted adversary in the group. The maximum trust level, an adversary is able to gain, is: $(k-1) \cdot \frac{\theta_{\max}}{\omega}$.

(3) **Malicious behavior.** If an adversary revocates a trustful member U_i, all issuers of trust assignments to U_i with a lower authorization level than the adversary have to renew their trust assignments towards U_i. Random revocating can thus result in a denial of service attack, leading members with low authorization levels to trigger the authentication process (with U_i) over and over again. Therefore, if their authentication process returns a positive result, the revocation of the adversary will be valued as misbehavior and the adversary's authorization level will be reduced.
The same applies for exaggerated reduction of authorization levels.

(4) **Revocation circumvention.** Trust assignments have a validity date (VD). When this date expires, the authentication process must be renewed (and a new trust assignment must be issued). Thus blocking of revocation assignments does work as long as the other trust assignments towards the adversary are not expired. Remark that trust and revocation assignments are broadcasted through the whole network, so blocking particular messages is not a simple task.

(5) **Adding virtual aversaries.** If one or a group of adversaries create virtual members, the authorization levels of these virtual members are bound by the adversaries' authorization levels, since the adversaries are the only group members who assign trust assignments to the(ir) virtual members. The adversaries impact on the whole mesh network is not raised due to their virtual members, since their own authorization level cannot be increased by their virtual members.
Nevertheless, the problem of virtual members cannot be removed nor detected (despite from some timing or physical aspects), if a virtual member simulates the normal behavior of a trustful mesh network member.

(6) **Denial of service.** To reduce the effect of denial of service when verifying bogus data, we propose RSA with a small public exponent as signature algorithm, since verification is very efficient in this case. Then, signature creation by a trustful user should only be done, if the requestor is authenticated successfully.
Further, all users U_i can make a guess (based on the validity date of their last sent trust assigment T_{ij} to user U_j), when the next request by U_j should

arrive. If the request is not received within this time range, U_i may deny to create a new trust assignment T_{ij}.

7 Evaluating the behavior of other nodes

In general, evaluating the behavior of other nodes and finding an appropriate trust estimation is not a trivial problem. Although we just have dealt with a general trust agreement solution in this paper, we want to outline shortly, how a behavior evaluation can look like.
There are two major cases to consider: A wireless mesh network with human interaction and an autonomously operated network.

With human interaction, trust assignments can be based on personal experiences with other network participants. This can be the case in community networks like SeattleWireless [2] or MIT Roofnet [1]. The trust opinion towards another user can be influenced by the confidentiality on the forwarded data, he provides. If your neighbor suddenly knows personal facts about you, that you have e.g. communicated via e-mail, you will probably lower his authorization level. Furthermore if you note that your data is not forwarded properly (maybe due to the ratio between forwarded and generated packets) or there is another misbehavior according to section 6, you will do the same. Increasing a trust level is done when noticing an ordinary behavior for a longer time period.

The case is much more complicated in an autonomously operated network, since there is no user interaction. Trust opinions can be based on non malicious behavior (see security considerations) and other actions that can be rated automatically. This is e.g. a reduced reliability when forwarding data, or the modification of data. In order to realize an automatic estimation of a neighbor's trust level, it is recommendable to deploy a local intrusion detection system (IDS).

8 Conclusion

We have presented the first trust agreement scheme that is especially designed for wireless mesh networks. The scheme can be operated in autonomous WMN to establish and maintain a trust relationship between the nodes of the network. Trust in wireless mesh networks consists of an authentication and an authorization part, whereby the first part is the number of nodes who authenticated a particular node and the latter part is used to value the behavior resp. misbehavior of a node.

An important part of our presented scheme is the introduction of abstract trust requirements for different positions of nodes in the network. Obviously, a node that forwards a lot of data from other nodes, needs more trust than a node that does not forward any data. Combining the new trust definition for WMN and the trust requirements, we propose a scheme that withstands a variety of attacks. An informal security proof concludes our contribution.

Future work is to analyze the behavior and misbehavior of mesh nodes in practice and to create rules for categorizing their behavior to be able to react with appropriate trust assignments. There is up to now no concrete proposal for an automated authentication process using a multifactor authentication (i.e. location based, fingerprint of public key, MAC address, hardware hash, etc.). Additionally it is open work to create more exact trust requirements for wireless mesh networks, as it is started in appendix A.1.

References

1. Mit roofnet, 2010. `http://pdos.csail.mit.edu/roofnet/doku.php`.
2. Seattlewireless, 2010. `http://www.seattlewireless.net`.
3. O. Cheikhrouhou, M. Laurent-Maknavicius, and H. Chaouchi. Security architecture in a multi-hop mesh network. 5th Conference on Safety and Architectures Networks SAR 2006, Seignosse, Landes, France, 2006.
4. Laurent Eschenauer. On trust establishment in mobile ad-hoc networks. Masterthesis, The Center for Satellite and Hybrid Communication Networks, 2002.
5. Laurent Eschenauer, Virgil D. Gligor, and John Baras. On trust establishment in mobile ad-hoc networks. In *LNCS 2845*, pages 47–66. Springer-Verlag, 2004.
6. S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651. ACM New York, NY, USA, 2003.
7. Yongdae Kim, Daniele Mazzocchi, and Gene Tsudik. Admission control in peer groups. In *NCA '03: Proceedings of the Second IEEE International Symposium on Network Computing and Applications*, page 131, Washington, DC, USA, 2003. IEEE Computer Society.
8. Xiaodong Lin, Xinhua Ling, Haojin Zhu, Pin-Han Ho, and Xuemin Sherman Shen. A novel localised authentication scheme in ieee 802.11 based wireless mesh networks. Int J. Security and Networks, Vol. 3, No. 2, pp. 122-132, 2008.
9. Rishab Nithyanand and Karthik Raman. Fuzzy privacy preserving peer-to-peer reputation management. Cryptology ePrint Archive, Report 2009/442, 2009. `http://eprint.iacr.org/`.
10. Andreas Noack and Stefan Spitz. Dynamic threshold cryptosystem without group manager. *International Journal of Network Protocols and Algorithms (ISSN: 1943-3581)*, 1(1):108–121, 2009.
11. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. ACM New York, NY, USA, 2000.
12. Benjamin Stritter and Tobias Wahl. Schlüsselverwaltung und -verteilung. Seminarwork, TU-Darmstadt, 2004.
13. Florian Walter. Authentifizierungsstrategien in mobilen adhoc-netzen. Seminarwork, Universität Tübingen, 2004.
14. Yanchao Zhang and Yuguang Fang. A secure authentication and billing architecture for wireless mesh networks. Wireless Networks, Vol. 13, No. 5, pp. 663-678, 2006.

A Extension for the Authentication Scheme

In this section, we give some proposals for the extension of the introduced trust agreement solution for mesh networks. We begin with an advanced abstract trust requirement scheme that allows a higher granularity.

A.1 Abstract Trust Requirements

It is obvious that nodes in the middle of the mesh network will forward more messages than nodes located at the margin. Given random pairs of nodes, the probability is above average (*Idea*: Pick a random node and partition the network into two halfs. The probability is $\frac{1}{2}$ that a second node is located in the other half. When picking n pairs of nodes, $\frac{n}{2}$ of them will communicate through the middle.) that they communicate through the middle.

Therefore it is smart to expect a higher trust from nodes in the middle of the mesh network than from nodes at the margin. For wireless mesh networks with internet gateways, this is even more complicated, since the communication will not be uniform as supposed in the former case. Nodes near the internet gateway and especially the internet gateway itself need a far higher trust requirement since they are forwarding the majority of the data. In addition to the introduced trust requirement values from section 4.2, we propose new values between "1" and "4": Nodes at the margin need less than "2", nodes in the middle need a trust level near to "3" and nodes in the near of an internet gateway need even more than "3". The internet gateway, however, should not have a trust level below "4".

A.2 Another Approach for computing global Trust

Definition 4 (section 4.4) shows how to compute a user's global trust value by summing up the particular local authorization levels and multiplying with the factor ω. This was the most obvious approach. However, there is a whole research field about optimizing trust aggregation e.g. in peer-to-peer, social networks and many more scenarios.

We head to the solution from Nithyanand et al. [9] who dealt with reputation management in peer-to-peer networks. They propose the ordered weighted average (OWA) function for the computation of the global reputation (global trust in our case). The advantage of this solution in comparison to our approach is that lower trust values become more weight, thus creating a more conservative scheme. We redefine Definition 4 as follows:

Definition 4*. *A user U_j's global trust value is computed as:*

$$(\alpha_j, \theta_j) := \Big(\sum_{\forall i : U_i \in S} \alpha_{ij}, \ \frac{\sum_{k=0}^{|S|} sort_k(\{\theta_{ij}\}, \forall i : U_i \in S) \cdot W_k}{s \cdot \sum_{k=0}^{|S|} W_k} \Big)$$

whereby S is the set of users U_i who issued valid trust assignments. s is the average number of ascertained trust assignments to the mesh nodes. The function $sort_k$ arranges all input values from the lowest to the highest value and returns the k'th element of this array.

Last but not least there is the weight function W undefined. In [9], the weight function W_k realizes that lower values have a higher impact. We present two alternatives for the weight function W:

$$W_k = W(k) = \sqrt[d]{|S| - k + 1}$$

whereby $d \in \boldsymbol{Z}_{>0}$. d lowers the impact of the weight function by moving the results closer to 1 and must be chosen in respect to the practical scenario.

The previous solution just achieves that lower values have a higher impact. Another approach is to weight the particular trust assignments by the relation of the transmitted authorization value and the maximum that could have been transmitted.

$$W = \frac{\theta_{ij}}{\theta_i}$$

To prevent recursions, θ_i must be assumed as a fixed value and may not depend on the global trust level of U_j (which is currently computed). If there is no value for θ_i yet, the maximum authorization value used in the network is used for θ_i. The advantage of this solution is that for each trust assignment the intention of the issuing user, whether this is a very positive or quite negative assignment, is included.

Actually, to provide even better results, both proposals can be combined.