Budapest University of Technology and Economics
Department of Telecommunications

Secure data forwarding in wireless multi-hop networks for mobile users

Collection of Ph.D. Theses
of
László Dóra

Research Supervisor:
Levente Buttyán, Ph.D.

Budapest, Hungary
2011

1 Introduction

In this thesis, I investigate security issues of two instances of multi-hop wireless networks: Delay Tolerant Networks and Wireless Mesh Networks.

A Delay Tolerant Network (DTN) is an infrastructureless network, where the message dissemination is performed by the participating mobile — usually battery driven — end-nodes. The messages are delivered in a *store-carry-and-forward* manner. With this approach, the messages can be delivered even if an online end-to-end route connecting the source and the destination never exists. This means that the intermediate mobile nodes carry the messages and pass them on to other intermediate nodes when they have a connection (e.g., when they are in vicinity).

I address some issues in delay tolerant personal wireless networks. These networks typically consist of handheld devices owned by mobile users and local information needs to be distributed to a set of nearby destinations based on their interest in the information.

Since in the considered application, the destinations are defined by their interests, the data packets are forwarded based on a dissemination approach. In dissemination based algorithms there is no a priori knowledge of possible routes towards the destination or destinations. Because of that and the fact that the destinations are not known either, each message must be disseminated all over the network. The basis of dissemination based algorithms is flooding, and they differ on how they limit the number of message copies.

I identified four security issues in delay tolerant personal wireless networks: 1) stimulating cooperation, 2) preventing SPAM, 3) providing fairness, and 4) preserving privacy.

A regular Wireless Mesh Network (WMN) consists of mesh routers (MR) that form a static wireless ad hoc network as an infrastructure and mesh clients (MC) that use that infrastructure. As mesh networks are typically not stand alone networks, some of the mesh routers function as gateways (GW) typically to the wired Internet. A subset of mesh routers function as wireless access points (AP) where mobile mesh clients can connect to the network. The sets of gateways and access points can overlap and they do not necessarily cover the entire set of mesh routers.

I concentrate on Wireless Mesh Networks, where the infrastructure is maintained by operators who provide broadband wireless access to the Internet for their customers based on contracts. The idea has gained increasing popularity (see e.g., Ozone's mesh network in Paris (`www.ozone.net`) and the Cloud in London (`www.thecloud.net`)).

In such networks, a novel approach is that the mesh routers are operated by multiple operators, and they cooperate in the provision of networking services to the mesh clients. This cooperation can be based on business agreements (similarly to roaming agreements in the case of cellular networks). Customers may be associated with one or more operators by contractual means and have the ability to roam to the rest of the cooperating operators, if necessary. The collaboration of multiple operators has some advantages (e.g., the installation cost can be reduced by using each other's networking elements).

The bandwidth can be increased using multiple interfaces and multiple channels in mesh routers. However, this approach requires special consideration in security design. Furthermore, WMNs have to support user mobility and they have to fulfill QoS requirements, too, because MCs can move during the data transmission while they may run QoS aware applications.

I refer to the above described Wireless Mesh Network, which is maintained by multiple operators, uses multiple interfaces with multiple channels, and supports user mobility and QoS, as Multi-WMN.

Three groups of main issues can be addressed regarding secure data forwarding in Multi-WMN: 1) fast authentication of MCs and access control to network resources, 2) protection of wireless communication including secure routing, and 3) intrusion and misbehavior detection and recovery.

2 Research Objective

In DTN, it is essential to prevent selfish behavior in data dissemination, because the data forwarding relies on the end-users' willingness to help each other. Current reputation and electronic payment solutions do not suit well the DTN environment. My main goal is to propose a distributed mechanism that encourages the nodes to store, carry, and forward messages even if they are not particulary interested in their contents. The mechanism should decrease the delivery delay and increase the delivery ratio.

I addressed the problem of traceability of users participating in DTNs. In this thesis, I investigate an issue specific to DTN arisen because of the store-carry-and-forward data delivery manner. In particular, an attacker can build a user profile of a node based on what messages the node stores and what messages it wants to download. After profiling, the attacker can trace the node even if the node communicates with the other nodes through anonymous links. I aim to propose a defense method against the above described attackers without jeopardizing the node's main goal, the message collection.

In Multi-WMN, I concentrate on the authentication and access control mechanism. My objective is to reduce the authentication delay, in order to support mobile users and seamless handover between the access points. Many proposed fast authentication schemes rely on trust models that are not appropriate in a multi-operator environment. In this thesis, my objective is to propose an authentication and access control method that satisfies all the requirements of Multi-WMNs.

I also address the problem of detecting misbehaving routers in Multi-WMNs and avoiding them when selecting routes. I consider misbehaving routers claiming fake information about their link or device properties in the control messages. Note that misbehaving routers may hold valid keys, and the authenticity of their messages is assured, thus, the receiving routers may utilize this information. Current solutions suffer from high overload or they do not suit multi-channel communication environment. My main goal is to propose a misbehaving router detection mechanism which can identify those routers that send fake information about their link states and device properties. Furthermore, I want to avoid to overload the network, and I require to suit the multi-channel environment.

3 Methodology

Before designing any methods, a list of requirements were assembled. The related proposals have been surveyed considering the requirement list. If none of them fulfilled all the requirements, a new method has been proposed. The methods were improved after the detailed analysis unless they meet all the requirements.

In each thesis group, I applied formal methods, simulations or measurements on real implementations in order to validate that the proposed solutions work as expected in the considered environment. When no real implementation has been prepared, a system model and an attacker model is built. The models are based on probabilistic and game theories.

In order to investigate the effectiveness of the proposed solutions, I define metrics which make it possible to compare my solutions to existing ones or to ideal or worst case scenarios. I used a Markovian model and probabilistic theories in order to show some properties of the metrics.

My analysis due to the complexity of the models are mainly based on extensive simulations. The investigation of the results rely on the average of multiple simulation runs and their empirical deviation or confidence interval. Realistic mobility models are considered thanks to SUMO mobility environment [SUM10] whose results are processed by C++ or Matlab based simulators.

4 New Results

4.1 Stimulating cooperation in data dissemination using barter in Delay Tolerant Networks

THESES 1: *In order to stimulate the cooperation in data dissemination, I propose barter as an exchange mechanism in Delay Tolerant Networks where messages are forwarded with a dissemination based approach. By means of simulations, I show that the proposed barter mechanism indeed encourages nodes to disseminate messages which results in faster delivery and higher delivery ratio. [C4] [J2]*

The problems identified in [PVS07] are the motivation for proposing a mechanism that encourages the users to carry other users' messages even if they are not directly interested in those messages. My proposed mechanism is based on the principles of *barter*: the users trade in messages and a user can download a message from another user if he/she can give a message in return. I expect that it is worth for the users to collect messages even if they are not interested in them, because they can exchange them later for messages that they are interested in. Thus, the messages are expected to propagate faster in the network.

THESIS 1.1: *I build a system model and run simulations in order to investigate the effects of selfishness in the considered Delay Tolerant Networks. I propose barter as an exchange mechanism in this context resulting in a novel approach which does not require any central entity as payment schemes do, nor the observation of other participants as reputation schemes require. Using game theory, I show that in a wide range of parameters of the simulations, the Nash Equilibrium strategies dictate that the users collect and disseminate messages even if they are not interested in them. This means that the proposed barter approach indeed mitigates the disadvantageous effect of selfishness. [C4] [J2]*

In my system model, a user and her device together is the *mobile node.* The messages are generated by special nodes called *message nodes.*

Each message has a type for each mobile node. A message is a primary message for a given mobile node, if the mobile node is interested in the content of the message and secondary if the mobile node is not.

A message has two main properties: the first one is the *popularity* (ζ) attribute and the second one is the *discounting characteristic* (δ). The popularity attribute describes the probability that a randomly taken mobile node is interested in the message. The discounting function determines the value of the messages over time. The secondary messages have no direct value for the nodes.

In my model, the mobile nodes are not able to exchange as many messages as they want but at maximum one message per time step. This limited exchange capability is called the *implicit cost* of the exchange, because there is no guarantee that the nodes can download all the messages that they want from the other party. In my system model, there is no other costs. However, the mobile nodes delete the messages from the memory whose value goes below a certain threshold D.

As shown in Eq. (1), the goodput ($0 \leq G_i(t) \leq 1$) for mobile node i at time t is the sum of the value of each primary message at the time of obtaining ($v_i(\tau)$) normalized with the value that node i could obtain in an ideal case ($|M_i^P(t)|$).

$$G_i(t) = \frac{\sum_{\tau=0}^{t} v_i(\tau)}{|M_i^P(t)|} \tag{1}$$

$v_i(\tau)$ is calculated from the discounting function as $v_i(t) = \delta(t - T_{m_i^t})$, where m_i^t is the message that mobile node i downloaded in time step t, T_m is the time step when message m was generated.

The goodput may vary over time, however it converges to a steady-state value as I prove in Thesis 1.3. Therefore, I will consider the goodput, denoted by G_i, of each mobile node i in the steady state.

$$G_i = \lim_{t \to \infty} G_i(t) \tag{2}$$

My approach to stimulate the cooperation of mobile nodes is based on the principles of *barter*. The mobile nodes exchange the same number of messages in a message-by-message manner, in preference order. In my model, the preference is based on the discounted value of the messages.

Recall that there is no direct benefit of downloading a secondary message. It is worth to download to exchange later for primary ones. According to this, the value of the secondary messages is considered only when a node defines its preference of messages during the message exchange. For a mobile node, secondary messages are worth $SP \cdot \delta(t)$ units time t after its generation. SP is called *secondary/primary ratio.* I have to emphasize that if $SP_u = 0$ then the mobile node u does not download any secondary messages.

I model my proposed mechanism as a game to analyze the behavior of the mobile nodes using game-theory. I define a non-cooperative game $G = [P, \{S_i\}, \{\pi_i\}]$, called *barter game.* P is the set of the players, S_i denotes the strategy space of player $i \in P$, and π_i represents the payoff function of each player i. To be more precise, π_i is the simplified notation of $\pi_i(s_0, s_1, ..., s_{|P|-1})$, because the payoff of each player depends on the strategy played by the other players.

In the barter game, the players (P) are the mobile nodes, and hence in the rest of this section, I will use the same notation for players as for mobile nodes. The strategy of each player is its secondary/primary ratio ($SP_i \in S_i = [0, 1]$). The players do not change their strategies during the game. The players choose their strategies in a way to maximize their goodput. Hence, the steady-state goodput is the payoff of the barter game for player i ($\pi_i = G_i$).

As one can see, the barter game is a symmetric game, because each player has the same strategy space ($S_0 = S_1 = ... = S$) and their payoff functions are equal ($\pi_i = \pi_j, i, j \in P$). A symmetric game G can be denoted by $[P, S, \pi()]$.

In the analysis of the barter mechanism, I am looking for the Nash Equilibria [FT91]. I limited ourselves to find only pure strategy, symmetric Nash Equilibria. In symmetric games, $\{s^*\}$ is Nash Equilibrium if the following equation holds for any player $i \in P$:

$$s_i^* = \arg\max_{s_i \in S} \pi(s_0^*, s_1^*, \dots, s_i, \dots), \text{where } s_u^* = s_v^* \forall u, v \in P/\{i\} \tag{3}$$

As one can see, it is easy to verify that a specific strategy profile $\{s'\}$ is a Nash Equilibrium or not. Considering any player $i \in P$ — without loss of generality $i = 0$, called *player NULL* — if it is worth for player i to deviate, $\{s'\}$ is not a Nash Equilibrium, whereas if s' is the best response to player i then s' will be the best response strategy for all the other players too, as the players have equal payoff functions. Therefore, to find the symmetric pure-strategy Nash Equilibria, investigation of a 2-dimensional space is enough. Thus, due to the symmetry of the game, the analysis is independent of the number of players.

Because of the complexity of the model, I use simulations instead of analytical tools. Therefore, I built a simulation environment in C++ where 300 mobile nodes move in discrete time steps according to one of the two mobility models: the Restricted Random Waypoint [BGLB02] and Simulation of Urban MObility [SUM10] model.

In Figure 1, where the best response of player NULL is plotted in a representative scenario, on the vertical axis, there are the strategies that player NULL can choose, while on the horizontal axis, the strategy space of the other players is placed. The Nash Equilibrium candidates are the

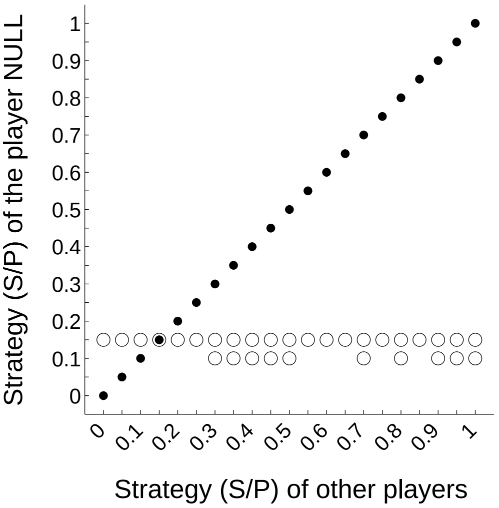


Figure 1: **Nash Equilibria in barter game**

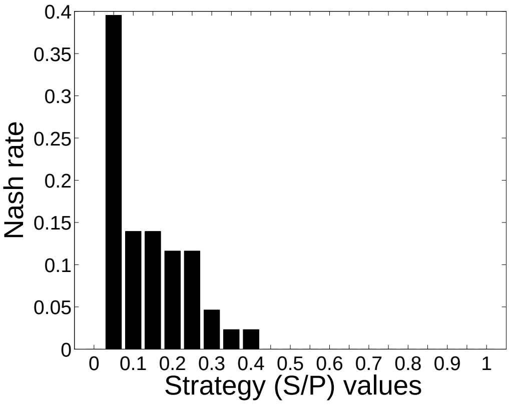


Figure 2: **Histogram of Nash Equilibrium values**

strategy profiles where player NULL and the other players choose the same strategy; these are denoted by solid, black points. Whereas, the best response strategy of player NULL to a specific strategy profile of the other players is denoted by empty circles. The Nash Equilibria are those $\{s\}$ values where the candidates match the best response function.

In Figure 2, the histogram of the Nash Equilibrium strategy values of all the considered simulation sets is plotted. The figure shows that in the simulated cases, the strategy which is most beneficial individually – the Nash Equilibirium of the barter game – to set the secondary/primary ratio to a low value but not to 0. Therefore, it is beneficial to help the other nodes ($s \neq 0$) carrying their messages when the nodes exchange messages in a fair manner.

THESIS 1.2: *I show by means of simulations that the barter mechanism when the nodes follow the Nash Equilibrium strategy increases the delivery ratio and speeds up the delivery in those scenarios from the considered ones when the selfish behavior hinders the message dissemination. Furthermore, I show that in some scenarios, the goodput is close to the ideal case. All these are performed by comparing three different cases: 1) one with barter as the encouraging mechanism where the users follow one of the Nash Equilibrium strategies, 2) one when the nodes store only those messages which they are interested in and no encouraging mechanism is present, and finally 3) one when all the users forward all the messages without any restrictions. [C4] [J2]*

In Figure 3, the goodput of the network is plotted against the popularity attribute value of the messages in three different scenario. The solid line refers to an upper bound for the goodput where the mobile nodes download all the new messages that they find in the memory of the connected node in one time step, both the primary and secondary ones. The line with dashes and dots refers to the goodput of the network when the nodes behave selfishly, in particular, they do not download any secondary messages, furthermore, there is no mechanism that encourages to do forward secondary messages. Finally, the line with dots refers to the goodput when the nodes are encouraged to store, carry, and forward messages with barter mechanism and they follow a strategy set according to the Nash Equilibrium of the barter game. In each simulations, the messages have the same popularity value. I present the 95% confidence intervals at each simulation points.

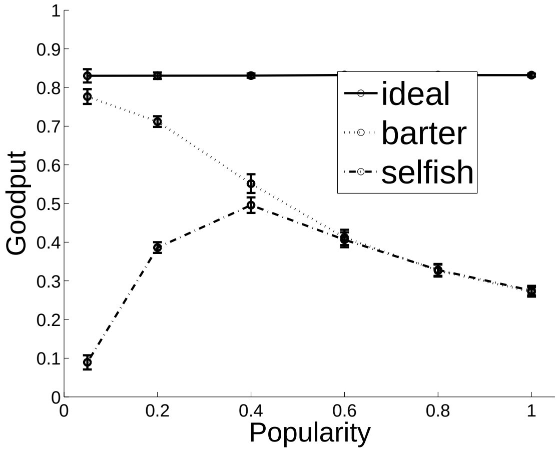


Figure 3: **Steady state goodput in ideal, selfish case and using barter**

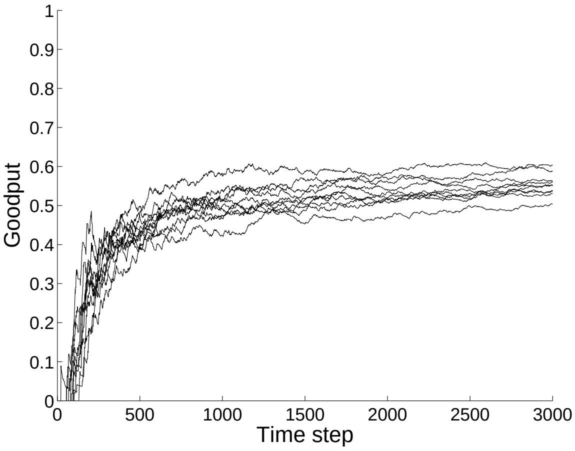


Figure 4: **The convergence of the goodput of some sample nodes**

As it can be seen, the barter mechanism increases the goodput in the networks where the popularity value of generated messages is low. Furthermore, in those cases, the goodput is close to the optimal goodput. Meanwhile, the barter mechanism does not decrease the goodput compared to the case when no encouraging mechanism present, but the nodes are willing to disseminate messages anyway. Note that with increasing message popularitiy, the goodput decreases, because in the considered cases the number of the messages that a node can obtain reaches earlier its upper limit while the number of the generated primary messages can increase higher when the popularity value increases.

THESIS 1.3: *In Theses 1.1 and 1.2, the investigations are based on a metric called goodput, which reflects the delivery ratio and the speed of data delivery simultaneously. The goodput is calculated by means of simulations, thus, it is critical to consider its steady state value. I show analytically using a Markovian model that the goodput converges to a steady state value at an exponential rate. Therefore, the goodput values would not change considerably in longer simulations, whose length are determined empirically [J2]*

In order to prove that the goodput converges to a limiting value as Figure 4 shows, I represented my system model as a finite state Markovian model. A state of the Markovian model can be described at time t as Eq. (4) shows.

$$\begin{aligned} s(t) = \{&B_1(t), B_2(t), \dots, B_N(t), \\ &Z_1(t), Z_2(t), \dots, Z_N(t), \\ &H_1(t), H_2(t), \dots, H_N(t)\} \end{aligned} \tag{4}$$

where

- N is the number of nodes
- $B_i(t) = [m_{i_1}, m_{i_2}, \dots]$ is the buffer of node i, where the messages are stored. The size of the buffer is 2^l, where l is the maximum length of the messages.
- $Z_i(t) \in \{*, m\}$ is the message stored in the memory of the message node i, where $*$ denotes the case when no message is stored at time t, otherwise m stands for the generated message, which arrives from a finite space of messages.

- $H_i(t)$ is the position of node i on field F where mobile nodes move.

Note, that the state space can be described by a deterministic mapping as Eq. (5) shows.

$$
\begin{aligned}
s(t+1) = \mathfrak{f}[s(t),& \\
& r_1(t+1), r_2(t+1), \dots, r_N(t+1), \\
& r'_1(t+1), r'_2(t+1), \dots, r'_n(t+1), \\
& r''_1(t+1), r''_2(t+1), \dots, r''_M(t+1)]
\end{aligned}
\tag{5}
$$

where $r_i(t+1)$, $r'_j(t+1)$, and $r''_k(t+1)$ refers to random elements that are the input for the next step of node i, for message generation at node j and for node pairing at meeting point k, respectively. The random numbers are generated independently of the time and of each other.

Note, that the state transition mapping is time independent. The sequence of state random variables $S(0), S(1), \dots, S(t), \dots$ constitutes a discrete time homogenous Markovian chain. The transition matrix of the Markovian process can be derived from Eqs. (4) and (5). An element P_{ij} of the transition matrix describes the probability that the system from state i change to state j.

A Markovian chain is *ergodic*, if $\lim_{n\to\infty} P_{ik}^{(n)} = P_k$ limiting value for each k exists, and the limiting values are independent of i and $\sum_{k=1}^{\infty} P_k = 1$.

As the classic theorem of Markovian chains claims, a finite state homogenous Markovian chain is ergodic, if it is irreducible and aperiodic. Particularly, there is a time step t and a state j, such that state j can be reached from arbitrary initial state i with positive probability with time step t. The convergence to limiting distribution P_j is exponential, which means the following: let $P_{ij}^{(t)}$ denote the probability, that the Markovian chain starting from state i arrives at state j with t steps, furthermore, let denote the stationary probability of state j by P_j, the difference $|P_{ij}^{(t)} - P_j|$ decreases exponentially when t tends to infinity (Theorem of Markov). In this case, uniform exponential bound exists for difference $|P_{ij}^{(t)} - P_j|$ independently of j.

In my model, the proof of the condition for ergodicity is the following: Assume the system is in an arbitrary state. I select a state k, let this state be the one where the buffer of the first node contains a single fresh message, while all other buffers are empty. Such a state can be reached from any other states in the following way: First, the buffers of the nodes become empty such that the users move or stagnate at a fixed position without meeting any message generator nodes. As the time passes the aging messages are dropped out from the buffer. Then the first node approaches a message node where it generates a fresh message and the node receives that message.

As it is shown above, my system is ergodic. The distribution of the stationary state is approached at exponential rate.

Considering Eq. (1), the goodput is affected by the transient state of the system also, not just on the stationary state. However, from the ergodicity of the Markovian chain, it follows that the effect of the transient state becomes negligible and fades away at an exponential rate if the time goes to infinity. By empirical observation, it is appropriate to consider the goodput after time step 3000 as the goodput will not change in the future considerably.

4.2 Hide-and-Lie for enhancing privacy in Delay Tolerant Networks

THESES 2: *For dissemination based Delay Tolerant Networks, I propose a method called Hide-and-lie in order to mitigate traceability of users. My proposal is beneficial against attacks where a user can be profiled based on the information on what messages the node stores and what messages it wants to download. Note that the users can be traceable even if each node communicates with the other nodes through anonymous links. [C6]*

The communication between the nodes can leak some information about the interests of the participants. In these theses, attacks based on these leaked information are considered.

THESIS 2.1: *I adopt the system model built in Theses 1, I build an attacker model, and I propose some specific attack algorithms for the considered Delay Tolerant Networks. I show by means of simulation that nodes are traceable in the considered model with high probability if no defense mechanism is applied. I investigate by analytical tools the limits of success probability of the attacks relying on the interest profile of the users. [C6]*

For the sake of simplicity, it is assumed that there are C categories, and each message belongs to a single category. A new message belongs to a specific category with probability $\frac{1}{C}$. A node is interested in any given category with probability ε. For the sake of simplicity, ε is equal for each node in each considered scenarios.

I assume that the attacker can estimate the following user profile (UP) from a node u at time t:

$$UP_u(t) = (EIP_u(t), CHM_u(t), IDL_u(t)) \tag{6}$$

where UP consists of the following triple:

- Estimated Interest Profile (EIP) is a binary vector. The value of the vector at the k^{th} position equals to 1 if category k seems to be interesting for node u.
- Category Histogram of offered Messages (CHM) shows, for each category, how many messages in the ID list belong to that category.
- IDL is the ID list of offered messages.

The attacker, in my model, behaves according to the following attacker model:

1. The attacker identifies its target node (u_T) from N nodes.
2. The attacker reads the current user profile of the target: $UP_{u_T}(t_0)$. The time step when this happens is considered as a reference time, i.e. t_0.
3. τ time later ($t_1 = t_0 + \tau$), the attacker reads $UP_{u_i}(t_1), i \in [1..N]$ of each node and calculates a metric how similar is u_i to u_T. τ is referred as the attacker delay.
4. The attacker chooses the node most similar to the target node. If more than one have the maximal similarity value, it chooses randomly between them. If the chosen node is u_T, the attacker is successful.

I have chosen for the analysis the success probability of the attacker as the privacy metric, because it is widely used and tells the most about the expected outcome of the attack.

Using the user profiles of the nodes, the attacker can calculate the similarity using an attacker function $\mathcal{A}$. More formally the input of $\mathcal{A}$ are $N+1$ user profiles, and the output is an ID of a node:

$$\mathcal{A} : (UP_{u_T}(t_0), UP_{u_i}(t_1), i \in [1..N]) \rightarrow j, j \in [1..N] \tag{7}$$

The attack is successful if and only if $j = T$.

It is clear that any attacker can reach a minimal value of the success probability $\frac{1}{N}$ by simple guessing. Higher values can also be achieved using more sophisticated attacker functions. In the following, four simple attacker functions are defined.

- **Prefiltered ID Based attacker function** The attacker can filter out every suspect who has different EIPs, considering only the nodes whose $EIP_u(t_1)$ equals to $EIP_{u_T}(t_0)$. From the remaining set, it selects the one whose $IDL_u(t_1)$ is the most similar to $IDL_{u_T}(t_0)$. Under similarity, the cardinality of the intersection of the target ID list and the suspect's ID list is meant.

- **Unfiltered ID Based attacker function** uses only the cardinality of the intersection of $IDL_{u_T}(t_0)$ and $IDL_u(t_1)$.

- **Category Histogram Based attacker function** selects the node u whose $CHM_u(t_1)$ is the most similar to the $CHM_{u_T}(t_0)$. The similarity of two histograms is calculated using the χ^2–test.

- **Significant Category Based attacker function** assumes that the interested categories are overrepresented in the ID list and the uninterested categories are underrepresented. To find the interested categories, the C categories is classified into the two clusters by using the k-means clustering algorithm [Har75] on the CHMs. The result of the clustering is a binary vector of length C with ones at the significant categories. The similarity of two binary vectors is defined as the Hamming distance of the vectors.

Even if an attacker can distinguish two nodes if their IPs are different (I call this attacker ideal IP based attacker $\mathcal{A}_{IP \text{ ideal}}$), the probability that two nodes have the same IP is not negligible. The success probability of an ideal IP based attacker can be viewed as an upper bound for any other IP based attacker, such as, e.g. the Significant Category Based attacker function. This value can be determined analytically.

The success probability of the ideal IP based attacker is determined by the number of equal IPs. To compute the success probability, first the probability p of two IPs being equal is computed as follows:

$$\begin{aligned} p &= \frac{\sum_{w=1}^{C} \binom{C}{w} \left(\varepsilon^2\right)^w \left((1-\varepsilon)^2\right)^{C-w}}{\left(1-(1-\varepsilon)^C\right)^2} \\ &= \frac{\left(\varepsilon^2 + (1-\varepsilon)^2\right)^C - (1-\varepsilon)^{2C}}{\left(1-(1-\varepsilon)^C\right)^2} \end{aligned} \tag{8}$$

where w is the weight of the IP varying between 1 and C (recall that every node is interested at least in one category).

The success probability of $\mathcal{A}_{IP \text{ ideal}}$ is the reciprocal of the average number of nodes with the same IP:

$$\begin{aligned} &\Pr(\mathcal{A}_{IP \text{ ideal}}(UP_{u_T}(t_0), UP_{u_1}(t_1), \ldots, UP_{u_N}(t_1)) = u_T) \\ &\simeq \frac{1}{1 + p\,(N-1)} \end{aligned} \tag{9}$$

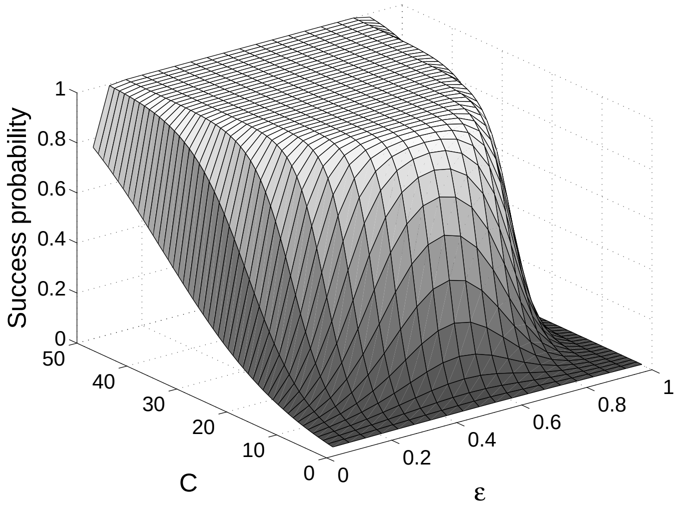


Figure 5: **Analytically determined upper bound for success probability of ideal IP based attacker functions**

In order to investigate the effectiveness of the proposed attacker functions, I run simulations, too. I consider different simulation parameters (e.g., different values for C and ε). The results are calculated from 100 simulation run in each parameter set.

The characteristic of the success probability of the attacker in the case of the considered scenario when no defense mechanism exist shown in Figure 6 where $\lambda = 0$ is similar to those which are simulated but not presented here. However, as Figure 5 shows, the success probability of the ideal IP based attacker depends on the parameter value of the number of categories (C) and the probability of a node being interested in a category (ε). As one can read from the figure, when there are large number of categories in the system, the success probability of an ideal attacker is high. On the other hand, when the number of the categories is low, the success probability highly depends on the value of ε. As the value ε gets closer to 0.5, the success probability increases. The reason is that an attacker can distinguish nodes when the probability that the IPs of two nodes are equal is low.

THESIS 2.2: *I propose a general defense mechanism, called Hide-and-lie against attackers considered in Thesis 2.1. I show by means of simulations that the success probability of the attacker can be decreased almost to the level of simple guessing while the goodput of the nodes does not decrease considerably, furthermore, in some scenarios, the goodput increases. [C6]*

In order to mislead the attacker, the nodes can slightly modify their UPs. Two simple methods can be used to modify the UP through modifying the Interest Profile (IP) of the node. The first one is to *hide* some interesting categories, and claim them as uninteresting. The second one is to *lie* about some uninteresting categories, and claim them as interesting. These techniques can be used at the same time, this is what I call *Hide-and-Lie Strategy* (HLS). The temporarily obfuscated IP is the Temporal Interest Profile or the EIP from the attacker point of view. The EIP can be transient, which means that a new EIP can be generated by every node in every time step.

Obviously, the required and offered messages during the message exchange must be synchronized with the EIP: 1) messages relating to hidden categories must be hidden as well and no message of hidden category should appear on request list, and 2) when a node lies about being

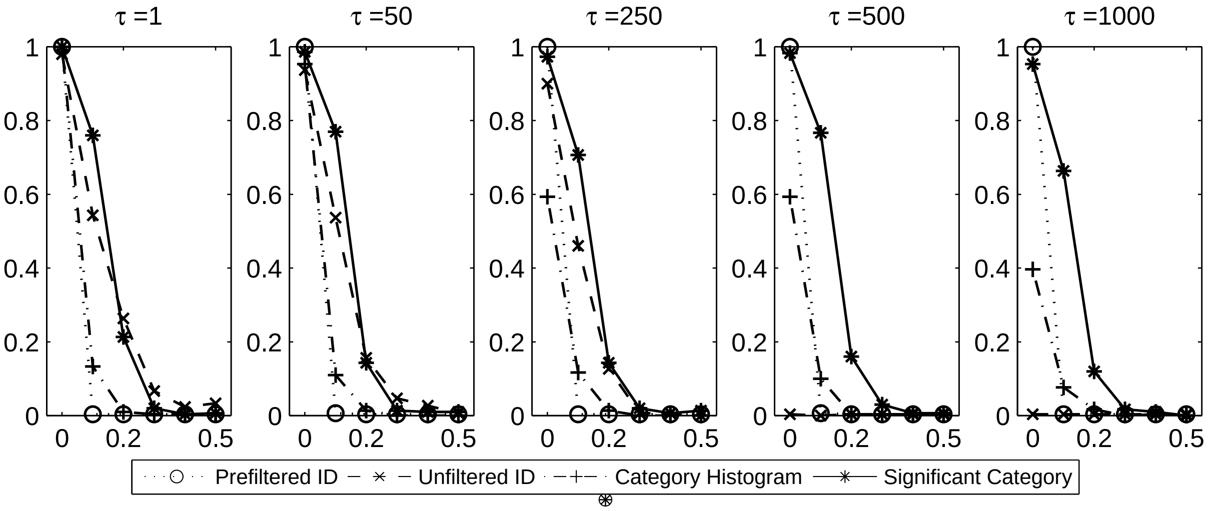


Figure 6: **Success probability of $\mathcal{A}$ as a function of the Hide-and-Lie strategy values (λ)**

interested in a given category, it collects and offers messages belonging to that uninteresting category.

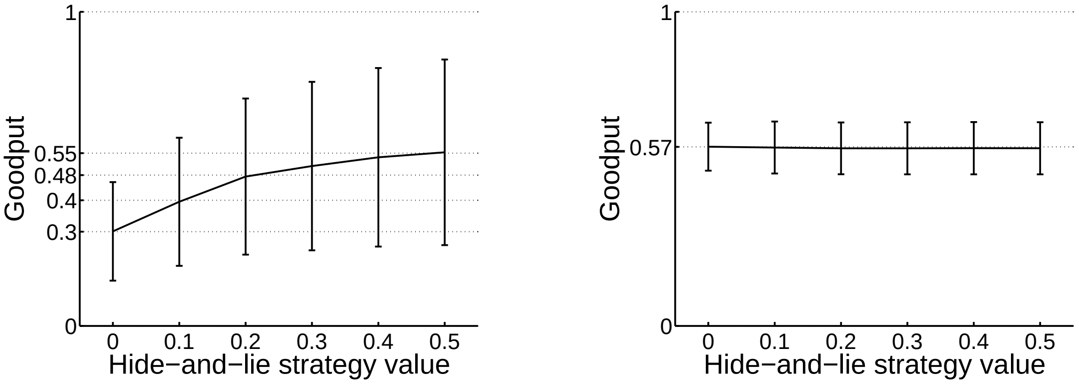
Every node generates its EIP from its IP by inverting every category in the IP with a given probability λ. Inverting means indicating an uninteresting category as interesting or vice versa. This parameter λ is the Hide-and-Lie strategy value.

The success probability of the attacker functions is plotted against different Hide-and-Lie strategy values (λ) and different attacker delay (τ) values in Figure 6. For the sake of better understanding, the plots are separated by different attacker delay values.

The Prefiltered ID Based attacker function is the most efficient attacker function when $\lambda = 0$, but in any other cases, it can not distinguish the target node from the others, because even one entry changing in the EIP misleads the attacker. The success probability of the Unfiltered ID Based attacker function decreases when $\lambda = 0$ compared to the prefiltered function but considerably increases when $\lambda > 0$. The Unfiltered ID Based attacker function is very sensitive for the attacker delay. The Category Histogram Based attacker function is less sensitive to the τ value, but it hardly tolerates that all the messages appear or disappear belonging to a category when EIP changes. The attack that is least sensitive to τ is the Significant Category Based attacker function. However, it still does not work when the nodes hide their identity with $\lambda = 0.5$ strategy, because there are no over- and underrepresented categories in that case.

Taking all the considered attacker functions into consideration, I found that a common tendency is that if the nodes apply the Hide-and-Lie Strategy with high value of λ, none of the attackers is able to distinguish them better, independently of the value of τ, than a naïve attacker which picks up one of the nodes by random.

In order to investigate the effect of the defense mechanism on the message delivery ratio, I defined the goodput here similarly to Eq. (1) in Theses 1. In Figure 7, I show the average goodput of all the nodes as a function of the Hide-and-Lie strategy in the two scenarios and its empirical standard deviation. I have to stress that these two figures do not represent all the appeared characteristic of the figures, however, Figure 7(a) shows an interesting property of the Hide-and-Lie Strategy. Namely, increasing λ does not degrade but increases the data delivery ratio in some scenarios. In Figure 7(b), the Hide-and-Lie strategy has no effect on the goodput.



(a) Scenario 1

(b) Scenario 2

Figure 7: **Average gain with the empirical standard deviation**

4.3 Fast authentication methods in multiple operator maintained Wireless Mesh Networks

THESES 3: *I propose two certificate based authentication and access control enforcement protocols for multi-operator maintained Wireless Mesh Networks which have some special requirements that current solutions do not fulfill. In order to reduce the authentication delay, I propose a so called weak key mechanism for constraint devices. [C3] [J1] [J3] [B1]*

In this section, I propose two certificate based authentication protocols for Multi-WMNs. First, I describe the architecture of the certificate based authentication protocols. Then, I investigate the speed characteristic of some classical crypto-primitives. After introducing a nonce-based and a timestamp-based authentication method, I define what public key algorithms and key sizes to use during the authentication in order to fulfill the general security requirements while still ensuring a short authentication delay during the handover. I also investigate the authentication delay in real environment.

THESIS 3.1: *I propose a certificate based authentication and access control enforcement protocol based on nonces. I show by measurements on a real implementation that the authentication delay does not cause intolerable interruption during the handover for the QoS aware applications in case of powerful mesh clients and constraint access points which is the typical case. I show informally that my solution fits to multi-operator maintained Wireless Mesh Networks. [J3]*

In my certificate based authentication and access control scheme, each operator operates its own certificate authority (CA). Each CA is responsible for issuing certificates for the access points belonging to the operator and issuing certificates to their subscribers. The CA also maintains the certificate revocation list (CRL).

The operators which decide to cooperate (O_1 and O_2) issue cross-certificates of their CAs. With the cross-certificates, entities (subscribers or access points) can perform certificate based authentication and key exchange mechanisms even if they belong to different operators.

The procedure of my nonce based authentication mechanism is shown in Figure 8, where ID_X, N_X, and K_X refers to the identity of, nonce and key generated by X, respectively (X can be AP or MC). $S_{P_X}(M)$ refers to digital signature calculated with X's private key over message M, while $E_{Q_X}(M)$ refers to encryption calculated with X's public key over message

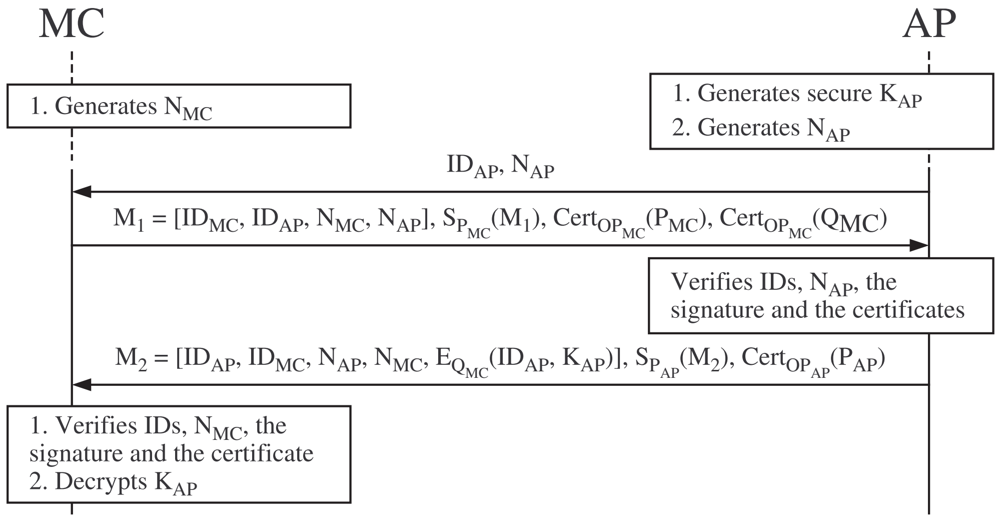

MC
AP
1. Generates N_{MC}
1. Generates secure K_{AP}
2. Generates N_{AP}
ID_{AP}, N_{AP}
$M_1 = [ID_{MC}, ID_{AP}, N_{MC}, N_{AP}], S_{P_{MC}}(M_1), Cert_{OP_{MC}}(P_{MC}), Cert_{OP_{MC}}(Q_{MC})$
Verifies IDs, N_{AP}, the signature and the certificates
$M_2 = [ID_{AP}, ID_{MC}, N_{AP}, N_{MC}, E_{Q_{MC}}(ID_{AP}, K_{AP})], S_{P_{AP}}(M_2), Cert_{OP_{AP}}(P_{AP})$
1. Verifies IDs, N_{MC}, the signature and the certificate
2. Decrypts K_{AP}

Figure 8: **Nonce based authentication**

M. $Cert_{OP_X(P_X)}$ denotes a certificate issued by X's operator that bounds the identity of X and its key.

Regarding the digital signatures and encryption, it is beneficial to shift as many computationally intensive operation to the MC as many possible, because of the following reasons: 1) Usually MCs which require seamless handover are more powerful than the APs, because they are ready to handle media streams. On the other hand, the MCs are usually constraint devices because they must remain cheap. 2) If the MC has to compute more, it increases the DoS resistance, as an attacker needs more investment to perform a successful DoS attack.

I take advantage of the fact that the two operations of some public key operations are asymmetric in respect of the time consumption. When the MC has more power than the AP (which is the typical case if I consider laptop computers as MCs), the MC can use RSA for digital signature, while the AP generates digital signatures with DSA. In that case all the computationally intensive operations (private key operations with RSA and digital signature verification with DSA) are shifted to the powerful MC, whereas, the lightweight operations are performed by the AP.

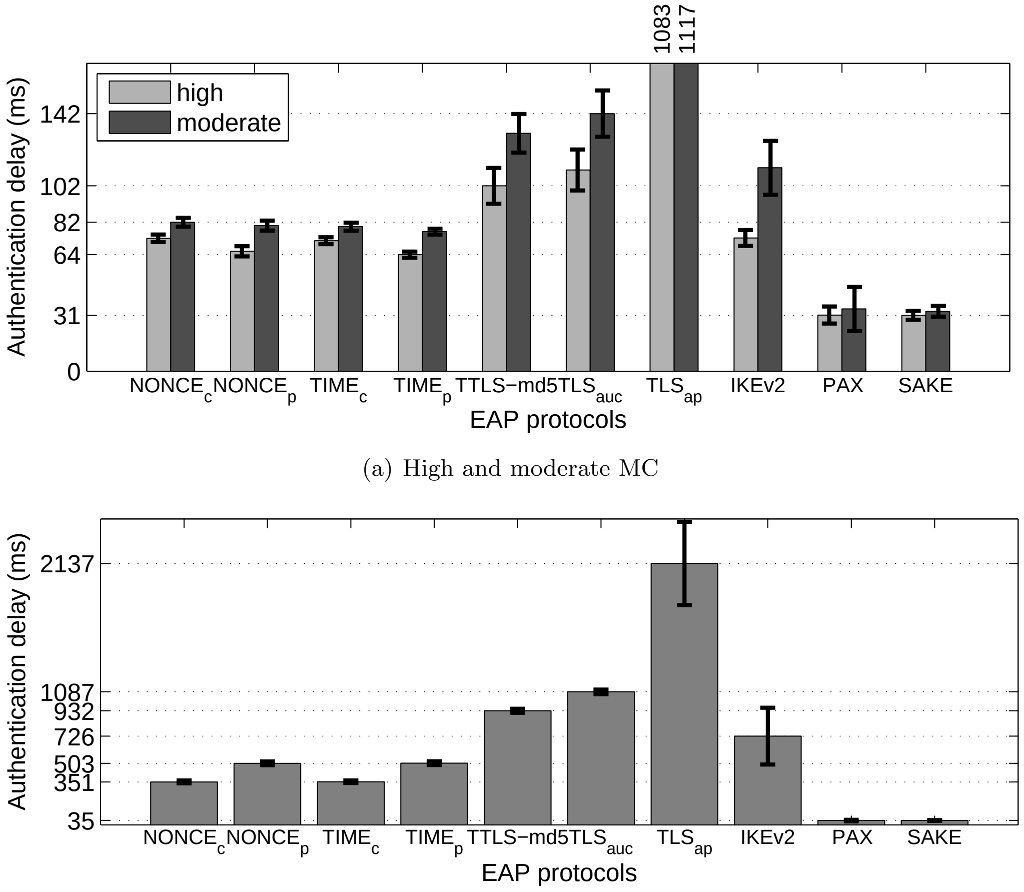
In order to ensure the confidentiality of the key K_{AP}, I propose to use minimum 1024 bit long keys. The public keys of the MCs are long-term keys. Therefore, I chose 1024 bit long public-private keys. The APs' public key are mid-term as they may change them frequently (e.g. daily). I also chose 1024 bit long keys for mid-term keys.

I created a proof-of-concept implementation. I embedded the authentication messages into EAP (Extensible Authentication Protocol) frames [ABV$^+$04]. EAP messages are embedded into EAPOL messages in IEEE 802.1X [IEE01] which is referred by IEEE 802.11i [IEE04] and IEEE 802.11r [IEE08], the current standard solutions for Wi-Fi authentication. The Pairwise Master Key (defined in IEEE 802.11i), which assures the access control enforcement, is calculated as $K_{conn} = Hash(K_{AP}, N_{MC})$ where $Hash()$ is a one-way function.

I investigated the authentication delay in different scenarios. In each case, the AP was a MikroTik Routerboard 133 with 175 MHz MIPS32 CPU. In order to analyze how the MC's performance affects the authentication delay, I used three different MCs: 1) high performance with 1.86 GHz 32 bit CPU, 2) moderate performance with 800 MHz 32 bit CPU, and 3) low performance with another MikroTik router.

I compared my proposal to classical, widely used solutions (e.g. EAP-TLS, EAP-TTLS) with authentication servers (AS). For these cases, I installed hostapd as a stand alone RADIUS [RWRS00] server on a powerful PC. In these scenarios, I connect the AS to the AP with direct link, thus, the roundtrip time between the AS and the MC is minimized.

I compared ten authentication scenarios with three different MC devices. I measured each case 100 times and calculated the average and the empirical standard deviation of the authentication delays. The results can be seen in Figure 9. On the horizontal axes, different protocols in different scenarios can be seen, while on the vertical axes, the authentication delay are shown. In each scenario, different bars correspond to the measurements made with different MC devices.



(a) High and moderate MC

(b) Constrained MC

Figure 9: **Average authentication delay with empirical standard deviation**

As one can see, the nonce based authentication method, referred as NONCE$_p$, significantly reduced the authentication delay compared to the centralized public key based authentication methods with the same key sizes (TTLS-md5, TLS$_{auc}$ and IKEv2). In these scenarios, the AS is a powerful entity in contrast to my mechanism where the AP has limited performance. In the scenario where the AS has such constraints as the AP (TLS$_{ap}$), the authentication delay is one order magnitude higher when TLS is used. The considered symmetric cryptography based solutions (PAX and SAKE) can complete in around 30-40 ms not taking into consideration the realistic value of the round trip time between the AP and a central authentication server. Note that the centralized solutions do not satisfy other requirements in the Multi-WMN.

My mechanism satisfies the regular requirements on the authentication in the QoS aware Wireless Mesh Networks because of the following reasons. Both the mesh client and the access point checks the authenticity of the other party, and the protocol assures for both participants

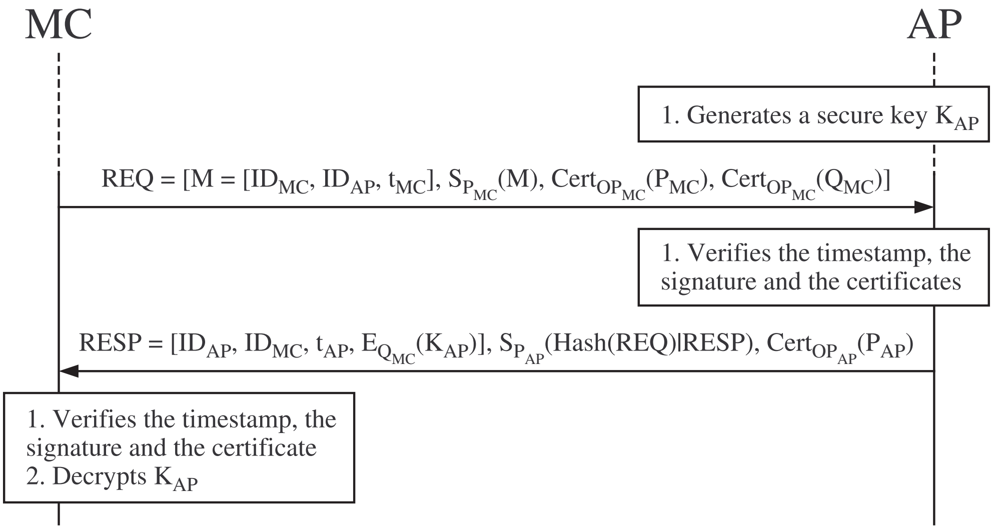

MC
AP
1. Generates a secure key K_{AP}
REQ = [M = [ID_{MC}, ID_{AP}, t_{MC}], $S_{P_{MC}}$(M), $Cert_{OP_{MC}}(P_{MC})$, $Cert_{OP_{MC}}(Q_{MC})$]
1. Verifies the timestamp, the signature and the certificates
RESP = [ID_{AP}, ID_{MC}, t_{AP}, $E_{Q_{MC}}(K_{AP})$], $S_{P_{AP}}$(Hash(REQ)|RESP), $Cert_{OP_{AP}}(P_{AP})$
1. Verifies the timestamp, the signature and the certificate
2. Decrypts K_{AP}

Figure 10: **Timestamp based authentication**

implicit key authenticity and key freshness. My solution is DoS resistant, and an attacker can defeat the access points only one by one. Furthermore, there is no central bottleneck because the authentication and the access control is distributed. Finally, my proposed scheme reduces authentication delay to an extent that makes seamless handover possible despite the usage of public key cryptography.

Meanwhile, my mechanism satisfies some special requirements of the multi-operator environment, too. The operators do not need to trust a single entity. The connection keys do not reveal any long-term keys, and the connection keys are independent of the previous and upcoming connections. With these solutions, the operators can protect themselves and their subscribers from the poorly set access points of other operators, and the weaknesses can be exploited by an attacker only locally.

I implement my proposals according to the EAP standard, therefore, it suits standard IEEE 802.11i and IEEE 802.11r. Consequently, my authentication scheme can be used both for inter- and intra-domain handovers.

THESIS 3.2: *I propose a certificate based authentication and access control enforcement protocol based on timestamps. I show by measurements on a real implementation that the authentication delay does not cause intolerable interruption during the handover for the QoS aware applications in case of powerful mesh clients and constraint access points which is the typical case. I show informally that my solution fits to multi-operator maintained Wireless Mesh Networks. [C3] [J3]*

The general advantages of timestamp based over the nonce based authentication methods are that the timestamp based solutions needs fewer random bits, and theoretically, mutual authentication can be performed with two messages in contrast to the nonce based solutions which requires three messages. In contrast to this, the timestamp based solutions require synchronized clocks. Note that the verification of the certificates requires loosely synchronized clocks, anyway. Therefore, no new requirement has to be met.

My timestamp based authentication scheme can be seen in Figure 10. The notations are the same as in Figure 8, the only new notation is the t_X, the timestamp sent by X (X can be AP or MC). The Pairwise Master Key is calculated as $Hash(K_{AP}, t_{MC})$.

Both the architecture and the usage of asymmetric cryptographic primitives are the same in case of the timestamp based solution as in the nonce based solution. Therefore, the statements in Thesis 3.1 hold for this thesis, too. In Figure 9, the method proposed here, when the same types of asymmetric cryptographic primitives and same key sizes are used, referred by TIME_p. The authentication delay is very similar to NONCE_p.

THESIS 3.3: *I propose a variant of the protocol proposed in Thesis 3.1 and 3.2 that allows constraint mesh clients to use shorter keys (weak keys). I show that a 30% reduction of authentication delay can be achieved by applying the weak key mechanism when constraint mesh clients are present. I show that the application of weak key mechanism is beneficial when the gain on the processing time of the public key cryptographic operations is larger than the loss on the longer certificate chain verification time.[C3] [J3]*

Note that a less powerful MC is not able to perform all the computing intensive operations. Therefore, I propose another technique to reduce the delay of the whole protocol at the cost of some pre-computation by both participants.

The idea is based on speeding up the digital signature operations using weak keys. The certificates belonging to weak keys have a very short lifetime, such that they surely expire by the time they will be broken.

The weak keys and the belonging certificates are generated by the participants before the handover happens. In fact, MCs and APs issue certificates themselves. First, it generates a weak public key pair. Then, it uses its identity as the name of the certificate and determines the expiration date which must be defined carefully, as the weak key can broken quickly. Finally, it supplies the certificate with digital signature using its private key, which is certified by the MC's operator for issuing certificates for weak keys. Therefore, any other entity who knows the CA's public key can validate the authenticity of the weak public key. The same mechanism can be performed at the AP side.

The validity of the certificates are short-term, therefore, maintaining of CRL is not required for implementing this mechanism. The certificates of the weak keys are signed with RSA so they can be verified very quickly.

I suggest to use 512 bit long keys as short-term keys which seems to be the best tradeoff for my purpose today between the validity time and the computational overhead. Similarly to the case of a powerful mesh client, the MC uses RSA and AP uses DSA to generate digital signatures.

The time synchronization needs to be performed in a secure way, otherwise an attacker can make a MC or AP to accept an already expired certificate of an already broken public key pair. However, the investigation of the secure time synchronization is out of scope of this thesis.

As one can see, in Figure 9(b), the weak key mechanism (referred by NONCE_c and TIME_c when applied to the nonce and timestamp based authentication methods, respectively) has significant benefit when the MC has low performance. The overall reduction of the authentication delay is around 30% on average in the considered scenario. However, as Figure 9(a) shows, the weak key mechanism increases the authentication delay when the MC has high or moderate performance.

In order to understand the reason that the authentication delay is increased in those cases, I investigate the effect of the weak key mechanism. From the reduction of the digital signature generation time (Δt_{gen}) and verification time (Δt_{verif}) both parties benefit, while the certificate verification delay (t_{cert}), and the transportation delay of the certificate of the weak key (t_{trav}) cause delay for both parties.

Taking these into consideration, in general, the usage of the weak key at one party is beneficial in my proposed authentication scheme if the Eq. (10) holds.

$$t_{cert}^{(B)} + t_{trav} < \Delta t_{gen}^{(A)} + \Delta t_{verif}^{(B)} \tag{10}$$

where A in upper index refers to the node that generates the certificate and B refers to the other party. Δt_{op} is the difference between the time consumptions of any operation op (gen or $verif$) with a long term key ($t_{op}(S)$) and with the weak key ($t_{op}(w)$) as Eq. (11) shows.

$$\Delta t_{op} = t_{op}(S) - t_{op}(w) \tag{11}$$

4.4 Misbehaving Router Detection in Link-state Routing for Wireless Mesh Networks

THESES 4: *I present a novel reputation system for detecting and avoiding misbehaving routers in Link-state Routing for Wireless Mesh Networks. [C1]*

My goal is to identify misbehaving routers at the data plane, and provide some feedback to the control plane that helps to avoid the identified misbehaving routers during the path selection procedure.

My misbehaving router detection protocol consists of three phases. In the first phase, called *traffic validation*, each gateway, which is assumed to be better protected physically than regular mesh nodes, and therefore, I assume that they behave correctly, collects information about the forwarding behavior of the routers on the paths belonging to the given gateway. In the second phase, called *router evaluation*, the gateways attempt to identify suspicious routers based on the traffic information collected in the previous phase. As a result of the router evaluation phase, the gateways compute Node Trust Values, and disseminate those within the network. Finally, in the third phase, called *reaction*, the routers select new routes by taking into account the Node Trust Values of the other routers.

THESIS 4.1: *I propose a novel reputation system for detecting misbehaving routers in Link-state Routing for Wireless Mesh Networks. Each router's reputation value is calculated over counters. Each router maintains a counter for each data flow and counts how many messages were forwarded in each flow. The counters are sent to the gateway that is at the end of the path. The gateway calculates a reputation value, called node trust value, for each router such that it counts on that a misbehaving router can send a fake counter value. I show by means of simulation that the proposed mechanism can differentiate misbehaving routers from honest ones. [C1]*

In order to support traffic validation, I require each node only to maintain a counter for each path it is part of to count the number of data packets that it forwards on a given path. I assume that each data packet has a routing header that contains a path identifier and message authentication codes. Thus, intermediate routers can verify the data packets and they count only intact packets. The packet counters that belong to a given path are requested by the gateway in a regular manner, and the routers on the path report them to the gateway.

As misbehaving routers may report fake counter values, the gateway does not use the reported counters directly in the computation of the Node Trust Values. Instead, the gateway considers different explanations for a set of received counter values. In each explanation, each intermediate router is either accused for misbehavior or considered honest, thus explanations are essentially binary vectors. The Node Trust Value of a given router is computed as a weighted sum of its accusations, where explanations that contain fewer accusations have higher weights. For the sake of simplicity, I assume that each link has high quality. Thus, the only reason for dropping a data packet is the malicious behavior of some routers in the data plane.

The upstream counter cnt^i of router i is meant to count the number of data packets that traverse router i. However, misbehaving routers may not correctly set their counters. Let us consider a simple case when a malicious router i is placed between two honest nodes. The attacker can set its counter to the number of incoming data packets cnt^i_{in} ($cnt^i = cnt^i_{in}$). In this case, the gateway realizes that on the link before the malicious router, there is no lost data packet as $cnt^i = cnt^{i-1}$. But on the next link, the difference is $cnt^{i+1} - cnt^i$. It is impossible to decide at the gateway side if node i indeed forwarded all the data packets and node $i+1$ dropped them, or node i dropped them, and node $i+1$ received only cnt^{i+1} data packets. Similarly, there are more explanations if the attacker sets its counter to the number of outgoing data packets cnt^i_{out} ($cnt^i = outcounter^i$).

In my attacker model, a malicious router sends the value of incoming counter as the traffic counter value with probability ξ and sends the value of outgoing counter with probability $1 - \xi$. I also investigate extreme cases when $\xi = 0$ and $\xi = 1$.

An explanation $\overline{exp}$ is a vector, where the i^{th} element of the vector is 0 if the i^{th} router in the route is assumed to be misbehaving — suspicious or accused in short —, otherwise, the i^{th} element is 1. An explanation is valid if all of the following statements hold:

- If there are data packets lost between node i and $i + 1$, at least one of them is accused.
- If node i and node j are not malicious in the given explanation, and there is no data packet loss between them, none of the nodes between i and j are accused.

Weights are assigned to each explanation of a counter report. I consider two kinds of calculation of the weights, both depends on the number of suspicious nodes in the explanation. Let us denote the number of suspicious nodes in explanation $\overline{exp}$ by $|\overline{exp}|$ and the number of all routers in the given path by $||\overline{exp}||$. The two different weight function $w_1()$ and $w_2()$ defined in Eqs. (12) and (13), respectively.

$$w_1(\overline{exp}) = q^{|\overline{exp}|} \cdot (1-q)^{||\overline{exp}||-|\overline{exp}|}, 0 < q \leq 1 \tag{12}$$

$$w_2(\overline{exp}) = \begin{cases} 1 & \text{if } |\overline{exp}| = \min_{\forall \overline{exp}_f}(|\overline{exp}_f|) \\ 0 & \text{else} \end{cases} \tag{13}$$

Using Eq. (13) as a weight function, I consider only those explanations which include the lowest number of suspicious nodes, the other explanations are discarded.

Given the set of possible explanations $\overline{exp}_e$ for a given set of counter reports, a gateway g which is one end of the route r calculates at time t the Node Trust Value of router i denoted by $\eta^{r(t)}_{i,g}$ in the following way:

$$\eta^{r(t)}_{i,g} = \sum_{\forall \overline{exp}_e} \frac{w(|\overline{exp}_e|)}{\sum_{\forall \overline{exp}_f} w(|\overline{exp}_f|)} \cdot \overline{exp}_e(i) \tag{14}$$

where each explanation $\overline{exp}_e(i)$ is weighted using the normalized value of one of the previously described weight function. Note, the $\eta^{r(t)}_{i,g}$ is always in the interval $[0, 1]$

In order to investigate the effectiveness of my solution, I run simulations with 200 mesh nodes placed uniformly at random in a two-dimensional field. Some of them are gateways and some of them are malicious.

In Figure 11, the Node Trust Value of three different groups can be seen with the 0.95 confidence intervals. The routers are categorized into three different groups: 1) malicious routers, 2) honest routers which are neighbors of malicious routers, and 3) other honest routers. I analyzed the latter two groups separately because the malicious routers can degrade the Node Trust Value of the neighboring nodes when the gateway evaluate the received upstream counters. At each group, four bars can be seen. The bars refer to different parameters of the malicious node detection mechanism. The `all` and `least` indicate the usage of Eq. (12) and (13), respectively. The `min` or `avg` indicates aggregation functions presented in Thesis 4.2.

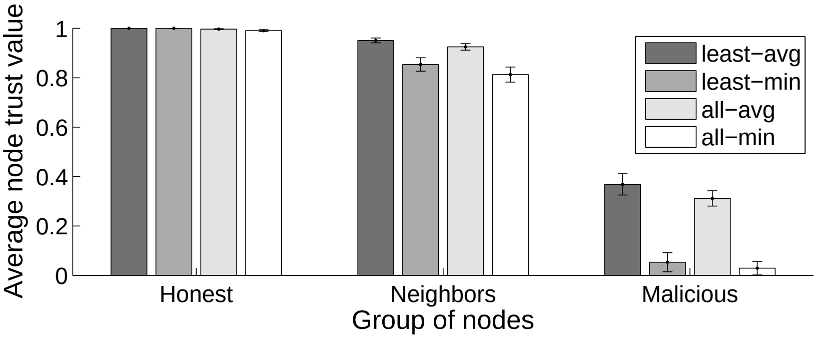


Figure 11: **Average Node Trust Value with 0.95 confidence intervals grouped by different node categories**

As Figure 11 shows, the Node Trust Value of the honest nodes is maximal. In contrast, the average Node Trust Value of the malicious nodes is significantly lower than the honest nodes' Node Trust Value. Considering the neighbors of the malicious nodes, the Node Trust Values are relatively high, but as I expected, significantly lower than of the other honest nodes. All in all, the malicious nodes can be bypassed in route selection with high probability if Node Trust Value is used for that purpose.

THESIS 4.2: *I propose a mechanism with which the routers are considered in the path selection procedure with a probability that is proportional to their node trust value presented in Thesis 4.1. I show by means of simulations that thanks to the detection and the route selection mechanism, the number of the dropped messages decreased around 50%, while the length of the routes increases only slightly. [C1]*

Note that a gateway may evaluate routers through multiple routes, and access points may receive multiple Node Trust Values from multiple gateways. Therefore, a mechanism for aggregation of Node Trust Values is required.

Each $\eta_{i,g}^{r(t)}$ are utilized using an n long window. These values may be calculated from different routes r_k or the same route but from different time t_l using function f. I investigate the minimum and the average function as f.

$$\eta_{i,g}^{(gw)} = f(\eta_{i,g}^{r_1(t_1)}, \eta_{i,g}^{r_2(t_2)}, \ldots, \eta_{i,g}^{r_n(t_n)}) \tag{15}$$

When access point a receives multiple $\eta_{i,g_k}^{(gw)}$ from different gateways g_k, it only stores the latest value from each gateway. The Node Trust Value that the access point calculates is denoted by $\eta_{a,i}^{(ap)}$ and calculated using the function f:

$$\eta_{a,i}^{(ap)} = f(\eta_{i,g_1}^{(gw)}, \eta_{i,g_2}^{(gw)}, \ldots, \eta_{i,g_m}^{(gw)}) \tag{16}$$

where m is the number of gateways that have sent Node Trust Value about router i.

Before the route selection, instead of considering all the routers, an access point determine a *subview* which the route selection runs on. Access point i includes router j into the subview with probability $\eta_{i,j}^{(ap)}$.

Note that with this approach, nodes in the subview may form a graph that is not connected, therefore, there is no guarantee that the access point can find any route to any gateway. If it happens, new subview generation is required. Nevertheless, in order to ensure that the procedure terminates, I define a threshold, which is initially 1, and the threshold decreases in each unsuccessful subview generation by ν. All the routers i for which $\eta_{a,i}^{(ap)} > 1 - r \cdot \nu$ are included in the subview (r is number of unsuccessful trials).

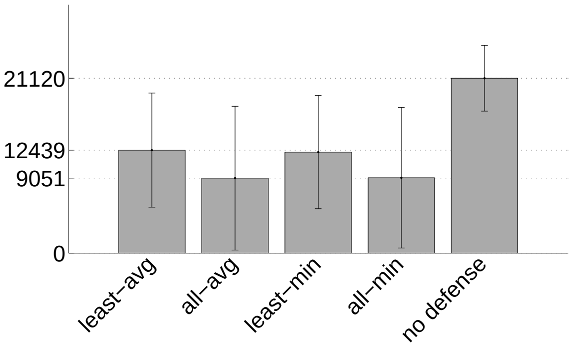


Figure 12: **Average numbers of dropped data packets with 0.95 confidence intervals**

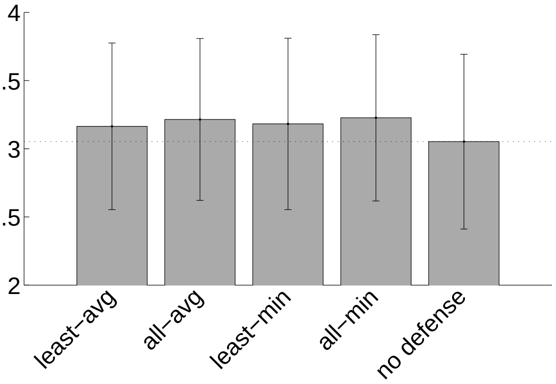


Figure 13: **Average lengths of the routes with 0.95 confidence intervals**

In Figure 12, the average number of dropped data packets are shown with 0.95 confidence intervals using different parameters of misbehavior node detection mechanism. These results are compared to the case when no defense mechanism is used at all. As one can see, the number of data packet drop is reduced with my mechanism considerably.

I also investigate the cost of avoiding malicious nodes by my mechanism. My simple QoS metric is the hop number. Thus, average length and the 0.95 confidence interval of the number of hops is shown in Figure 13. As one can see, the length of routes does not increase significantly with my mechanism. This comes from the fact that in many cases, the access points could choose alternative routes which had the same length as the route that contained malicious routers, too.

5 Application of New Results

In this thesis, two instances of multi-hop wireless networks are considered: 1) Delay Tolerant Networks, and 2) Wireless Mesh Networks. Different issues are investigated in each instance. In this section, the application of new results presented in this thesis is described.

Regarding the Delay Tolerant Networks, I imagined a scenario where local information needs to be distributed to a set of nearby destinations based on their interest in the information. These networks consist of handheld devices belonging to individual mobile users.

For disseminating information among tourists, instead of setting up an on-line bulletin board, where the tourists have to pay both for the usage of bulletin board service and for accessing the network, a city-wide Delay Tolerant Network can provide a very cheap alternative solution. In this solution, touristic information can be distributed in a store-carry-and-forward manner by using Bluetooth capable devices (e.g., mobile phones, PDAs) and by exploiting the mobility of the tourists themselves.

In Vehicular Ad hoc Networks (VANET), the cars communicate with each other in order 1) to provide higher safety and/or higher permeability for the traffic, or 2) to entertain the passengers. In order to satisfy some special requirements of VANET, current design principles require roadside infrastructure. However, due to the high price of the roadside infrastructure installation, in the sparsely built-up areas, the vehicles can only communicate with each others with DTN approach. Considering the entertainment applications in VANET, usually it is not worth to build up any infrastructure, therefore, the vehicles will probably communicate with each other according to DTN approach, too.

In the typical DTN scenarios as described above, the end users are responsible for the data forwarding due to the lack of the infrastructure. DTN networks compared to infrastructure based networks promise cheap but not reliable data forwarding. Reliability can be increased by motivating the users to forward each others' messages. Considering an extreme situation, if none of the users forward messages on behalves of other users, messages are destinated only when the source and the destination nodes meet each other. In practice considering the above described examples, it could mean that 1) tourists learn that a museum is closed when they go to the museum, and 2) a car receives information about an accident when it is close to the accident instead of at a fork in the road where the accident can be bypassed easily on an alternative route. The barter based solution encourages users to disseminate messages on behalves of other nodes making reasonable to supplement infrastructures with DTN approach.

The traceability also can be an issue in DTN networks. Due to the fact that the end users store and forward the message while they are moving, the users could become traceable if the message forwarding protocol is not designed carefully. Considering the tourist example, if the tourists are traceable, they can be targeted by advertisements based on the information what place they visit. Also in VANET networks, the privacy should not be violated. Anonymous communication has been investigated in the context of mobile ad hoc networks, too. But there is a DTN specific problem due to the store-carry-and-forward data dissemination manner. In particular, users can be profiled based on the information that they store and they want to download. The Hide-and-Lie solution is proposed in order to prevent attackers to trace the nodes who apply the solution.

The barter and Hide-and-Lie proposals and their investigation was applied to BIONETS (BIOlogically inspired NETwork and Services) EU project. The FP6 project aimed to develop an infrastructureless network providing evolutionary services that adapt to the users' needs automatically at the service layer. The project started in 2006 and successfully ended in February of 2010. More information can be found at `http://www.bionets.eu`.

The investigation of both barter and Hide-and-Lie mechanisms were delivered to BIONETS as technical reports. Furthermore, the barter mechanism was integrated to the BIONETS

Simulator. BIONETS Simulator is an OMNeT++ based simulator through which the results of the whole project were presented in an integrated form.

Wireless Mesh Networks provide last mile broadband access for mobile users who may run QoS aware applications. Maintaining them by multiple operators could be advantageous even if the operators compete with each other. Furthermore, the multi-channel approach with multiple wireless interfaces could have high gain for the operators.

The novel fast certificate based authentication method proposed for multi operator maintained Wireless Mesh Networks can be utilized by mobile business users who require access to corporate services and real time multimedia applications for work while they are traveling. The employee effectiveness can be improved and the companies can take advantage of these applications if the network access is cheap as the Wireless Mesh Network promises. However, business users require the same level of quality of services as for the 3G connections. Therefore, re-authentication of the users at new access points is essential, but the process could have intolerable delay. Especially when the access point where the mobile business user associated belongs to other operator than the previous access point.

For the certificate based fast authentication method, I proposed the weak key mechanism. Note that this mechanism can be applied to any protocols where the delay of digital signatures is critical and only the authenticity of the messages must be assured, but not non-repudiation. As a particular example, this mechanism was applied when routing messages were flooded in the network using digital signatures. The performance of generating and verifying digital signatures was increased with the weak key mechanism.

The performance of the certificate based authentication method and the weak key mechanism was evaluated through real implementation. I used the context of hostapd and wpa_supplicant [Mal09] to embed my authentication messages to EAP format. Therefore, in IEEE 802.11 wireless networks, these mechanisms can be used with minor implementation improvements.

I proposed a misbehaving router detection mechanism for link-state routing protocols. The main advantage of the proposal is — in contrast to some current solutions — that it does not require the routers to keep their neighbors under observation during the message forwarding phase, which may have low performance in a multi-channel environment. My mechanism has been implemented in the framework of OLSRd [ols10], too.

Misbehaving router detection mechanism can be applied to e.g., video surveillance application. The owners of block of houses may use video surveillance in order to track illegal activities. Thanks to the cheap installation of Wireless Mesh Networks, owners may choose a solution based on mesh routers that transmit the picture of cameras to the monitoring room through wireless hops. The behavior of mesh routers can be modified by an external attacker due to the lack of physical protection. An attacker who gets control over a mesh router can achieve by falsifying the routing metrics that the wireless cameras forward the pictures through the misbehaving routers. An attacker can prevent delivering the pictures to the computer which should store the data by simply dropping all the messages. During the attack, any kind of illegal activities can be done without getting nabbed. Misbehavior of the mesh routers must be detected in order to provide reliable video surveillance.

Fast authentication methods and misbehaving router detection mechanism were delivered to an EU project dealing with multi-operator maintained Wireless Mesh Networks. The EU project was launched in FP7 called EU-MESH (`http://www.eu-mesh.eu`). The project started in 2008, and successfully ended in the third quarter of 2010.

References

[ABV$^+$04] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard), June 2004. Updated by RFC 5247.

[BGLB02] Ljubica Blažević, Silvia Giordano, and Jean-Yves Le Boudec. Self organized terminode routing. *Cluster Computing*, 5:205–218, April 2002.

[FT91] D. Fudenberg and J. Tirole. *Game Theory.* MIT Press, 1991.

[Har75] J.A. Hartigan. *Clustering algorithms.* John Wiley & Sons, Inc. New York, NY, USA, 1975.

[IEE01] IEEE Std 802.1X-2001. IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control, June 2001.

[IEE04] IEEE Std 802.11i™. Medium Access Control (MAC) security enhancements, amendment 6 to IEEE Standard for local and metropolitan area networks part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications., July 2004.

[IEE08] IEEE 802.11r™-2008. IEEE Standard for Information Technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 2: Fast BSS Transition, July 2008.

[Mal09] Jouni Malinen. WPA/RSN Supplicant (wpa_supplicant) and WPA/RSN/EAP Authenticator (hostapd) v0.6.7. `http://hostap.epitest.fi/`, 2009.

[ols10] olsrd. an ad hoc wireless mesh routing daemon, 2010. `http://www.olsr.org`.

[PVS07] Antonis Panagakis, Athanasios Vaios, and Ioannis Stavrakakis. On the Effects of Cooperation in DTNs. In *Proc. of The Second IEEE/Create-Net/ICST International Conference on COMmunication System softWAre and MiddlewaRE (COMSWARE)*, pages 1–6, January 7-12 2007.

[RWRS00] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865 (Draft Standard), June 2000. Updated by RFCs 2868, 3575, 5080.

[SUM10] SUMO. Simulation of Urban MObility. `http://sumo.sourceforge.net/`, 2010.

6 Publication of New Results

Book Chapters

[B1] I. Askoxylakis, B. Bencsáth, L. Buttyán, L. Dóra, V. Siris, and A. Traganitis. *Cross-layer security and resilience in wireless mesh networks.* Cross Layer Designs in WLAN Systems, Troubador Publishing Ltd, Emerging Communication and Service Technologies Series, 2010.

International Journal Papers

[J1] I. Askoxylakis, B. Bencsáth, L. Buttyán, L. Dóra, V. Siris, D. Szili, and I. Vajda. Securing Multi-operator Based QoS-aware Mesh Networks: Requirements and Design Options. *Wireless Communications and Mobile Computing (Special Issue on QoS and Security in Wireless Networks)*, 10(5):622–646, 2009.

[J2] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter Trade Improves Message Delivery in Opportunistic Networks. *Elsevier Ad Hoc Networks*, 8(1):1–14, January 2010.

[J3] L. Buttyán, L. Dóra, F. Martinelli, and M. Petrocchi. Fast Certificate-based Authentication Scheme in Multi-operator maintained Wireless Mesh Networks. *Elsevier Computer Communications*, 33(8):907–922, April 2010.

International Conference and Workshop Papers

[C1] G. Ács, L. Buttyán, and L. Dóra. Misbehaving Router Detection in Link-state Routing for Wireless Mesh Networks. In *Proceedings of the Second IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMESH'10)*, Montreal, Canada, June 2010.

[C2] A. Bohák, L. Buttyán, and L. Dóra. An User Authentication Scheme for Fast Handover Between WiFi Access Points. In *Proceedings of the Third Annual International Wireless Internet Conference*, Austin, Texas, USA, October 22-23 2007. ACM. (invited paper).

[C3] L. Buttyán and L. Dóra. An Authentication Scheme for QoS-aware Multi-operator maintained Wireless Mesh Networks. In *Proceedings of the First IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMESH'09)*, Kos, Greece, June 2009.

[C4] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter-based cooperation in delay-tolerant personal wireless networks. In *Proceedings of the First IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications.* IEEE Computer Society Press, June 2007.

[C5] L. Buttyán, L. Dóra, and I. Vajda. Statistical Wormhole Detection in Sensor Networks. In *Proceedings of Security and Privacy in Ad-hoc and Sensor Networks: Second European Workshop*, pages 128–141, Visegrad, Hungary, July 13-14 2005. Springer-Verlag GmbH.

[C6] L. Dóra and T. Holczer. Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking ACM/SIGMOBILE MobiOpp 2010*, Pisa, Italy, February 22-23 2010.

National Journal Papers

[N1] L. Buttyán and L. Dóra. Wifi biztonság - a jó, a rossz, és a csúf. *Híradástechnika*, May 2006.

Theses

[T1] D. László. Féregjárat detektálása szenzorhálózatokban statisztikus eszközökkel. Master's thesis, Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar, 1111 Budapest, Egry József u. 18., May 2005.

Other

[O1] D. László. Féregjárat detektálása szenzorhálózatokban statisztikus eszközökkel. TDK III. helyezet, November 2004. Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar.

Citations

[J2] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter Trade Improves Message Delivery in Opportunistic Networks. *Elsevier Ad Hoc Networks*, 8(1):1–14, January 2010.

is cited by

[1] A. Mei and J. Stefa. Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals. In *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, pages 488–497. IEEE, 2010.

[C2] A. Bohák, L. Buttyán, and L. Dóra. An User Authentication Scheme for Fast Handover Between WiFi Access Points. In *Proceedings of the Third Annual International Wireless Internet Conference*, Austin, Texas, USA, October 22-23 2007. ACM. (invited paper).

is cited by

[1] Liang Cai, S. Machiraju, and Hao Chen. Capauth: A capability-based handover scheme. In *INFOCOM, 2010 Proceedings IEEE*, pages 1 –5, March 2010.

[2] Zoltán Faigl, Stefan Lindskog, and Anna Brunstrom. Performance evaluation of ikev2 authentication methods in next generation wireless networks. *Security and Communication Networks*, 3(1):83–98, 2010.

[C3] L. Buttyán and L. Dóra. An Authentication Scheme for QoS-aware Multi-operator maintained Wireless Mesh Networks. In *Proceedings of the First IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMESH'09)*, Kos, Greece, June 2009.

is cited by

[1] Bing He. *Architecture Design and Performance Optimization of Wireless Mesh Networks.* PhD thesis, University of Cincinnati, Ohio, 2010.

[C4] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter-based cooperation in delay-tolerant personal wireless networks. In *Proceedings of the First IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications.* IEEE Computer Society Press, June 2007.

is cited by

[1] Panayotis Antoniadis. *Mobile Peer-to-Peer Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications*, chapter Incentives for Resource Sharing in Ad Hoc Networks: Going Beyond Rationality, pages 218–239. IGI Global, 2009.

[2] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan, and Mehran S. Fallah. A secure credit-based cooperation stimulating mechanism for manets using hash chains. *Future Generation Computer Systems*, 25(8):926 – 934, 2009.

[3] I. Koukoutsidis, E. Jaho, and I. Stavrakakis. Cooperative content retrieval in nomadic sensor networks. In *INFOCOM Workshops 2008, IEEE*, pages 1 –6, April 2008.

[4] Udayan Kumar, Gautam Thakur, and Ahmed Helmy. Protect: proximity-based trust-advisor using encounters for mobile societies. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, IWCMC '10, pages 636–645, New York, NY, USA, 2010. ACM.

[5] G. Resta and P. Santi. The effects of node cooperation level on routing performance in delay tolerant networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, pages 1 –9, June 2009.

[6] Xiaojuan Xie, Haining Chen, and Hongyi Wu. Bargain-based stimulation mechanism for selfish mobile nodes in participatory sensing network. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, pages 1 –9, June 2009.

[7] Xiong Yong-Ping, Sun Li-Min, Niu Jian-Wei, and Liu Yan. Opportunistic Networks. *Journal of Software*, 20(1):124–137, 2009.

[C6] L. Dóra and T. Holczer. Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking ACM/SIGMOBILE MobiOpp 2010*, Pisa, Italy, February 22-23 2010.

is cited by

[1] Iain Parris and Tristan Henderson. Privacy-enhanced social-network routing. *Computer Communications*, In Press, Corrected Proof:–, 2010.

[C5] L. Buttyán, L. Dóra, and I. Vajda. Statistical Wormhole Detection in Sensor Networks. In *Proceedings of Security and Privacy in Ad-hoc and Sensor Networks: Second European Workshop*, pages 128–141, Visegrad, Hungary, July 13-14 2005. Springer-Verlag GmbH.

is cited by

[1] Marianne Azer, Sherif El-Kassas, and Magdy M. S. El-Soudani. A full image of the wormhole attacks - towards introducing complex wormhole attacks in wireless ad hoc networks. *CoRR*, abs/0906.1245, 2009.

[2] Marianne Azer, Sherif El-Kassas, Abdel Wahab Hassan, and Magdy El-Soudani. Intrusion detection for wormhole attacks in ad hoc networks: A survey and a proposed decentralized scheme. *Availability, Reliability and Security, International Conference on*, 0:636–641, 2008.

[3] Marianne A. Azer, Sherif M. El-Kassas, and Magdy S. El-Soudani. A scheme for intrusion detection and response in ad hoc networks. In Houda Labiod and Mohamad Badra, editors, *New Technologies, Mobility and Security*, pages 507–516. Springer Netherlands, 2007. 10.1007/978-1-4020-6270-4-42.

[4] Marianne A. Azer, Sherif M. El-Kassas, and Magdy S. El-Soudani. Immuning routing protocols from the wormhole attack in wireless ad hoc networks. *Systems and Networks Communication, International Conference on*, 0:30–36, 2009.

[5] Zhu Bin, Liao Jun'guo, and Zhang Huifu. Defending wormhole attack in aps dv-hop. In *Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on*, pages 219 –224, August 2008.

[6] Kasper Bonne Rasmussen and Srdjan Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, pages 331 –340, September 2007.

[7] Hyeon Choi and Tae Cho. Energy efficient mac length determination method for statistical en-route filtering using fuzzy logic. In De-Shuang Huang, Kang-Hyun Jo, Hong-Hee Lee, Hee-Jun Kang, and Vitoantonio Bevilacqua, editors, *Emerging Intelligent Computing Technology and Applications*, volume 5754 of *Lecture Notes in Computer Science*, pages 686–695. Springer Berlin / Heidelberg, 2009. 10.1007/978-3-642-04070-2-74.

[8] Tassos Dimitriou and Athanassios Giannetsos. Wormholes no more? localized wormhole detection and prevention in wireless networks. In Rajmohan Rajaraman, Thomas Moscibroda, Adam Dunkels, and Anna Scaglione, editors, *Distributed Computing in Sensor Systems*, volume 6131 of *Lecture Notes in Computer Science*, pages 334–347. Springer Berlin / Heidelberg, 2010. 10.1007/978-3-642-13651-1-24.

[9] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, and Xiangke Liao. Topological detection on wormholes in wireless ad hoc and sensor networks. In *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*, pages 314 –323, October 2009.

[10] Dezun Dong, Mo Li, Yunhao Liu, and Xiangke Liao. Wormcircle: Connectivity-based wormhole detection in wireless ad hoc and sensor networks. *Parallel and Distributed Systems, International Conference on*, 0:72–79, 2009.

[11] Jing Dong, Kurt E. Ackermann, Brett Bavar, and Cristina Nita-Rotaru. Mitigating attacks against virtual coordinate based routing in wireless sensor networks. In *Proceedings of the first ACM conference on Wireless network security*, WiSec '08, pages 89–99, New York, NY, USA, 2008. ACM.

[12] Jing Dong, Kurt E. Ackermann, Brett Bavar, and Cristina Nita-Rotaru. Secure and robust virtual coordinate system in wireless sensor networks. *ACM Trans. Sen. Netw.*, 6:29:1–29:34, July 2010.

[13] S.M. Glass, V. Muthukkumarasamy, and M. Portmann. Detecting man-in-the-middle and wormhole attacks in wireless mesh networks. In *Advanced Information Networking and Applications, 2009. AINA '09. International Conference on*, pages 530 –538, May 2009.

[14] Stephen Mark Glass, Vallipuram Muthukkumarasamy, and Marius Portmann. Detecting man-in-the-middle and wormhole attacks in wireless mesh networks. *Advanced Information Networking and Applications, International Conference on*, 0:530–538, 2009.

[15] Rennie Graaf, Islam Hegazy, Jeffrey Horton, and Reihaneh Safavi-Naini. Distributed detection of wormhole attacks in wireless sensor networks. In Ozgur Akan, Paolo Bellavista, Jiannong Cao, Falko Dressler, Domenico Ferrari, Mario Gerla, Hisashi Kobayashi, Sergio Palazzo, Sartaj Sahni, Xuemin (Sherman) Shen, Mircea Stan, Jia Xiaohua, Albert Zomaya, Geoffrey Coulson, Jun Zheng, Shiwen Mao, Scott F. Midkiff, and Hua Zhu, editors, *Ad Hoc Networks*, volume 28 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 208–223. Springer Berlin Heidelberg, 2010. 10.1007/978-3-642-11723-7-14.

[16] Thaier Saleh Hayajneh. *Protocols for Detection and Removal of Wormholes for Secure Routing and Neighborhood Creation in Wireless Ad Hoc Networks.* PhD thesis, University of Pittsburgh, 2009.

[17] Jinsub Kim, Dan Sterne, Rommie Hardy, Roshan K. Thomas, and Lang Tong. Timing-based localization of in-band wormhole tunnels in manets. In *Proceedings of the third ACM conference on Wireless network security*, WiSec '10, pages 1–12, New York, NY, USA, 2010. ACM.

[18] Fan-rui Kong, Chun-wen Li, Qing-qing Ding, Guang-zhao Cui, and Bing-yi Cui. Wapn: a distributed wormhole attack detection approach for wireless sensor networks. *Journal of Zhejiang University - Science A*, 10:279–289, 2009. 10.1631/jzus.A0820178.

[19] Hae Young Lee and Tae Ho Cho. A report generation method for defending false negative attacks in ubiquitous sensor networks. *International Journal of Computer Science and Network Security*, 7(11):49–54, 2007.

[20] Hae Young Lee and Tae Ho Cho. Statistical en-route filtering of fabricated reports in ubiquitous sensor networks based on commutative cipher. *International Journal of Computer Science and Network Security*, 8(3):216–221, 2008.

[21] Hae Young Lee, Tae Ho Cho, and Hyung-Jong Kim. Fuzzy-based detection of injected false data in wireless sensor networks. In Samir Kumar Bandyopadhyay, Wael Adi, Tai-hoon Kim, and Yang Xiao, editors, *Information Security and Assurance*, volume 76 of *Communications in Computer and Information Science*, pages 128–137. Springer Berlin Heidelberg, 2010. 10.1007/978-3-642-13365-7-13.

[22] Hae Young Lee, Soo Young Moon, and Tae Ho Cho. Adaptive false data filtering method for sensor networks based on fuzzy logic and commutative cipher. In *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*, pages 228 –232, December 2008.

[23] Sanjay Madria and Jian Yin. Serwa: A secure routing protocol against wormhole attacks in sensor networks. *Ad Hoc Networks*, 7(6):1051 – 1063, 2009.

[24] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux. Secure neighborhood discovery: a fundamental element for mobile ad hoc networking. *Communications Magazine, IEEE*, 46(2):132 –139, February 2008.

[25] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. *Asia-Pacific Conference on Services Computing. 2006 IEEE*, 0:172–178, 2007.

[26] Eric Platon and Yuichi Sei. Security software engineering in wireless sensor networks. 2008.

[27] Marcin Poturalski, Panos Papadimitratos, and Jean-Pierre Hubaux. Secure neighbor discovery in wireless networks: Is it possible? Technical Report EPFL-LCA Report 2007-004, Ecole Polytechnique Fdrale de Lausanne, 2007.

[28] Marcin Poturalski, Panos Papadimitratos, and Jean-Pierre Hubaux. Towards provable secure neighbor discovery in wireless networks. In *Proceedings of the 6th ACM workshop on Formal methods in security engineering*, FMSE '08, pages 31–42, New York, NY, USA, 2008. ACM.

[29] B. Prasannajit, Anupama S. Venkatesh, K. Vindhykumari, S.R. Subhashini, and G. Vinitha. An approach towards detection of wormhole attack in sensor networks. *Integrated Intelligent Computing*, 0:283–289, 2010.

[30] Reza Shokri, Marcin Poturalski, Gael Ravot, Panos Papadimitratos, and Jean-Pierre Hubaux. A practical secure neighbor verification protocol for wireless sensor networks. In *Proceedings of the second ACM conference on Wireless network security*, WiSec '09, pages 193–200, New York, NY, USA, 2009. ACM.

[31] Reza Shokri, Marcin Poturalski, Gael Ravot, Panos Papadimitratos, and Jean pierre Hubaux. A low-cost secure neighbor verification protocol for wireless sensor networks. 2008.

[32] Ajit Singh and Kunwar Singh Vaisla. A mechanism for detecting wormhole attacks on wireless ad hoc network. *International Journal of Computer and Network Security*, 2(9):27–31, 2009.

[33] D. Sterne, G. Lawler, R. Gopaul, B. Rivera, K. Marcus, and P. Kruus. Countering false accusations and collusion in the detection of in-band wormholes. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pages 243 –256, December 2007.

[34] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Ttm: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, pages 593 –598, January 2007.

[35] T. Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. In *Asia-Pacific Service Computing Conference, The 2nd IEEE*, pages 172 –178, December 2007.

[36] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao, and Rishav Khemka. A graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks. *International Journal of Recent Trends in Engineering (IJRTE)*, 1(2):220–222, 2009.

[37] Xia Wang. Intrusion detection techniques in wireless ad hoc networks. In *Computer Software and Applications Conference, 2006. COMPSAC '06. 30th Annual International*, volume 2, pages 347 –349, September 2006.

[38] Xia Wang. Intrusion detection techniques in wireless ad hoc networks. *Computer Software and Applications Conference, Annual International*, 2:347–349, 2006.

[39] W. Znaidi, M. Minier, and J.-P. Babau. Detecting wormhole attacks in wireless networks using local neighborhood information. In *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, pages 1 –5, September 2008.