# Quantitative Safety and Security Analysis from a Communication Perspective

Boris Malinowsky
Telecommunications Research Center Vienna (FTW), Austria
malinowsky@ftw.at

Hans-Peter Schwefel
FTW, Austria &
Aalborg University, Denmark
hps@kom.aau.dk

Oliver Jung
Telecommunications Research Center Vienna (FTW), Austria
jung@ftw.at

## ABSTRACT

This paper introduces and exemplifies a trade-off analysis of safety and security properties in distributed systems. The aim is to support analysis for real-time communication and authentication building blocks in a wireless communication scenario. By embedding an authentication scheme into a real-time communication protocol for safety-critical scenarios, we can rely on the protocol's individual safety and security properties. The resulting communication protocol satisfies selected safety and security properties for deployment in safety-critical use-case scenarios with security requirements. We look at handover situations in a IEEE 802.11 wireless setup between mobile nodes and access points. The trade-offs involve application-layer data goodput, probability of completed handovers, and effect on usable protocol slots, to quantify the impact of security from a lower-layer communication perspective on the communication protocols. The results are obtained using the network simulator ns-3.

## Categories and Subject Descriptors

C.2.5 [**Local and Wide-Area Networks**]: Ethernet (e.g., CSMA/CD); C.4 [**Performance of Systems**]: Performance attributes; I.6 [**Simulation and Modeling**]: Miscellaneous

## Keywords

real-time protocol, wireless communication, authentication, safety & security

## 1. INTRODUCTION

In many use-case scenarios, nodes exhibit mobility patterns that require them to communicate wirelessly. When such networked components communicate over wireless links, they provide a broader attack surface for malicious nodes in gathering information and executing security exploits. One challenge in enforcing security properties of a system is that existing security countermeasures might conflict with design aspects of safety-critical systems. Distributed systems with safety-critical requirements demand for reliable communication services with timely response and for high service availability. This is specified in the communication system via upper time bounds for message delivery and redundancy concepts, and realized via messaging protocols satisfying worst-case execution times, and the selection of specifically certified robust hardware components, amongst others. In resource-constrained environments like embedded systems deploying wireless technologies, the contributors for time delay can be distinguished as processing and transmission time. The latter is the evaluation focus of this paper.

With authentication, we refer to the procedure of ensuring message origin authentication i.e., verifying its origin. For messages, the necessary information carried for authentication is referred to as message integrity code (MIC). Authentication has several practical applications, e.g., it is a prerequisite for access control to networks, or (re-)authentication in handover situations of mobile nodes to a different Access Point (AP). Those applications can have adverse effects to meeting real-time requirements for communication. Messaging protocols for safety-critical application domains are often required to disseminate state information or alerts in a multicast fashion, with high probability of message delivery. Here, receivers either have to authenticate the AP wirelessly distributing the message, and—upon establishing authenticity—implicitly trust the sending node, or directly perform authentication on the origin sender.

### 1.1 The Safety & Security View

From a traditional point of view, a common approach during system design is the isolated study and validation of safety and security properties. When embedding security features into a safety case, the challenge is to identify conflicts caused by the combined safe and secure design. But methodologies used to either assess safety or security aspects are often not adequate for a joint evaluation of safety and security interdependencies. Methods for determining the security, and the aim of increasing the assurance into a system, are usually based on risk assessment approaches. The overall assumptions differ from the point of safety versus security. When establishing safety properties, usually a closed system design is assumed, while security properties apply to open connected systems. Besides the danger that the initial assumption of a closed system might not be correct, the increased use of open communication systems in safety-critical systems requires an understanding of the mutual impact of safety and security mechanisms. This allows to identify the trade-offs for system design and configura-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
VALUETOOLS 2014, December 09-11, Bratislava, Slovakia
Copyright © 2015 ICST 978-1-63190-057-0
DOI 10.4108/icst.valuetools.2014.258185

tion. Further, quantifying those trade-offs enables more accurate reasoning about system properties, and integrating those findings for tool support. Authentication as a security attribute is a system property, and appropriate measures are required to quantitatively use them together with stochastic simulation approaches for safety [8]. To allow discussion of synergy effects and cross-influences, system designers need a methodology that jointly addresses the analysis of safety and security properties. A list of possible conflicts where security does not support the safety case is shown in Table 1. With the focus on embedded systems, platforms are resource constrained, e.g., in processing power, and do often not include dedicated hardware with security functionality to keep costs down. Traditionally, to meet safety and availability requirements, systems often use proprietary (custom-designed) components, while the approach of deploying Commercial Off-The-Shelf (COTS) components for security functions is commonly accepted. Several impacts can be observed. A positive impact, where security supports safety, is that it prohibits unauthorized components on interfering with system safety during operation. Negative impacts are a) the introduction of additional components for authentication, those need to be included from a safety perspective, b) higher network traffic, e.g., packet size, required hand-shake procedures for authentication, session updates, and c) increase in time delays, e.g., during node handover. The goal is to have a common evaluation of selected safety and security blocks for the purpose of exchanging messages in a safety-critical system with security requirements.

We provide a quantitative characterization of security and safety impacts on wireless communication in embedded systems and resource-constrained environments for mission-critical applications. The focus of our analysis is on results obtained from a stochastic simulation setup. We are interested in simulating a worst-case scenario with saturated channels that will cause higher delays and retransmissions of our real-time protocol. For simulation we are using ns-3. Exemplary results are shown for the IEEE 802.11 4-way handshake [1] in comparison to TV-HORS [11].

The paper is outlined as follows: Section 1.3 describes a use-case scenario for our network architecture. Section 2 discusses conflicts of safety and security for the case of wireless communication, and summarizes the selected real-time protocol and authentication mechanisms (Sections 2.1 and 2.2). Section 2.2.2 describes the signature scheme for efficient multicast authentication called TV-HORS we compare to WPA2. The analysis in Section 3 exemplifies derived quantitative communication metrics.

## 1.2 Related Work

The authors of [8] discuss techniques for a quantitative, model-based evaluation for dependable and secure systems. They also look into approaches involving discrete event simulation like network simulation tools, and the need to quantify system properties for security. The case of security as a safety issue, and the need to combine safety and security in safety-critical infrastructures of railways systems is discussed in [10]. The paper shows the trend to integrate existing communication technologies into railway communication, and the challenge to part with traditionally closed systems. An analysis of a train control system is given in [6], focused on availability and failure modeling. The authors of [4] address the same problem as our paper, discussing the security impact on a safety case. Their method for assessing the security risks associated with a system such as a large-scale critical infrastructure differs by iterating on Claims-Arguments-Evidence (CAE). There exist several approaches and improvements for authentication based on one time signatures. Besides the one applied by us [11], Chang et al. propose improvements for efficient broadcast authentication in wireless sensor networks [5]. An approach and tool for modeling safety and security interdependencies via Boolean logic Driven Markov Processes (BDMP) is shown in [9], following the analysis method known from fault and attack trees. For the selected real-time protocol from [7], that paper also contains experimental measurement setups for IEEE 802.11. Our paper differs in regarding both safety and security requirements for a combined model to better understand the merits of such evaluation method.

Table 1: Possible Conflicts for Safety & Security [3]

| **Safety** | **Security** |
|---|---|
| Timeliness | Encryption and authentication |
| Limited resources | Encryption and authentication |
| Redundancy | Confidentiality |
| Closed trust model | Open trust model |
| Continuous operation through upgrades | Up-to-date security patches |
| Extensive use of proprietary systems | Extensive use of COTS |

## 1.3 Scenario

The use-case scenario for the assessment described in Section 3 are metropolitan area networks (MANs), with a first-hop wireless link from a mobile node to the infrastructure. One example is the communication system for metropolitan railways, with data exchanged as unicast and multicast. In the selected communication setup, a mobile node resembles a train cabin moving on railway tracks, maintaining communication with a control station via APs alongside the track. Communication requirements between cabin and infrastructure include upper temporal bounds for message delivery, and message resilience. The infrastructure is based on IEEE 802.11 WLAN [1]. In such a setup, regular handover occurs of the mobile node to APs in the perimeter with overlapping coverage zones. As the APs provide a public external surface for access, protocol nodes need to authenticate.

# 2. SAFETY & SECURITY MECHANISMS

One trade-off in safety versus security for real-time communication and authentication is the increase of required resources for authentication. First, processing times might delay the real-time protocol time schedule, up to violating requirements of upper communication time bounds. Second, authentication tasks cause interruption of communication services. Third, the authentication data overhead can result in scalability problems, e.g, by the increase in messaging (by redundancy in the time and information domain). Those issues can be categorized as a) concerns of availability, i.e.,

readiness for service, and b) data integrity, regarding data corruption, omission and delivery, and c) reliability regarding transmission. Based on those categories and the applied strategies for reliable communication, embedding the selected authentication mechanism into our communication protocol leads to the following trade-offs. The combined design provides authenticity, but negatively affects:

- Bandwidth: the message size increase negatively affects any combination of a) max. allowed application-layer data, b) available redundancy in time, i.e., the message resilience degree, c) information redundancy, e.g., additional error detection or data duplication.
- Redundancy in Space: multiple communication links also have to cope with interleaving authentication procedures to avoid interruption of service, introducing a common cause fault.

These two points affect the worst-case under which a system is resilient to degrading conditions of communication over unreliable wireless links. Taking a look at the trade-offs, we can partially study them from a quantitative perspective by detailing the wireless communication environment, technologies, and faults. This provides the basis to apply our methodology of using a discrete event network simulator to address those points in question.

Wi-Fi Protected Access (WPA) as a standardized mechanism for node authentication has two main drawbacks: 1) it requires a handshake Station–AP before continuing with communication. While this ensures the attribute of security (node authenticity), it severely lengthens the handover procedure, which affects the readiness for service (availability). Examples of quantitative comparison later in this paper show that effect. The second mechanism TV-HORS is selected being an efficient multicast authentication scheme. Authentication usually requires an initial key exchange or initialization phase. For TV-HORS, this is the case for the regular exchange of new keychains between mobile node and the APs. This causes considerable data overhead during operation, and needs to be weighed against other protocol advantages. The main benefit is that the handover procedure to the next selected AP is limited to association only. In the following we summarize the selected real-time protocol TRC and the authentication mechanisms WPA2 and TV-HORS.

## 2.1 Safety: TRC Protocol

The Timed Reliable Communication (TRC) protocol [7] is specifically designed for operation over wireless links in safety-critical scenarios. The protocol provides synchronous and time-bounded communication for IEEE 802.11 compliant devices that are Quality of Service (QoS) enabled, i.e., support IEEE 802.11e. The devices use the Distributed Coordination Function (DCF) mode. The protocol design aims at applications with low bandwidth requirements. It enforces strict upper bounds on Worst Case Execution Times (WCETs), for distribution of broadcast, multicast, and unicast messages. Messages are assigned a criticality level, parametrized based on the required probability of message delivery, and realized as a bound on the maximum retransmissions of a message. The overall communication architecture follows a centralized communication setup. The setup uses the notation of a coordinator, with all communication distributed via the coordinator. The coordinator maintains the allocation of necessary communication resources among its node set, and executes the communication schedule for the nodes. The schedule uses communication rounds and fixed node time slots. During a round, the coordinator polls each node of the node set in a predetermined order. In each time slot, the associated node is polled by the coordinator, with the node sending a request back to the coordinator (containing status information or a new message for distribution), and the coordinator broadcasts to its node set. The coordinator continually updates its view of whether a node of the set has received a message or not.

The protocol is based on the assumption that an upper bound exists on the number of consecutive message losses for the target environment. If no status update is received from a node (after a poll) for more than a specific number of times, the coordinator considers that node to have left the connected node set. The nodes and the coordinator execute detectors that timely decide on message omission (and therefore, absent nodes), as well as nodes deviating from the expected execution behavior.

The coordinator itself is a logical unit. For our purposes, this coordination mechanism is replicated in the access points, to coordinate the associated nodes. The assumption of the backbone infrastructure is a fast wired network, e.g., a closed system with a high-speed redundant fiber ring topology. For coordination, any updates of AP node sets, messages for wireless transmission, and delivered messages are distributed/collected over that backbone without considerable loss or delay.

## 2.2 Security: Authentication Schemes

We here shortly outline both WPA2 and TV-HORS.

### *2.2.1 WPA2*

The Wi-Fi Protected Access II (WPA2) is an implementation of IEEE 802.11i merged into [1]. As part of a Robust Security Network Association (RSNA) establishment, temporal key exchange takes place by executing a key management algorithm, as specified in Section 8.5.3 of [1]. That protocol is called the 4-way handshake, and completes the IEEE 802.1X authentication process, see Figure 1.

In detail, the supplicant (station or node) and the authenticator (AP) can either use a Master Session Key (MSK) or a Pre-Shared Key (PSK) to derive a Pairwise Master Key (PMK). Creating a master session key as common secret, the overall process involves the supplicant, the authenticator, and optionally an authentication server for security capability discovery and 802.1X conversations. Having the PMK, the 4-way handshake protocol is executed for RSNA establishment. This produces a Pairwise Transient Key and a Group Transient Key, subsequently shared by the supplicant and authenticator for Unicasts and Multicasts, respectively.

*QoS Management Frames.* A handshake is executed using the EAPOL (Extensible Authentication Protocol over LANs) frame type. As with the frame type for association (management frame), QoS header information as initially

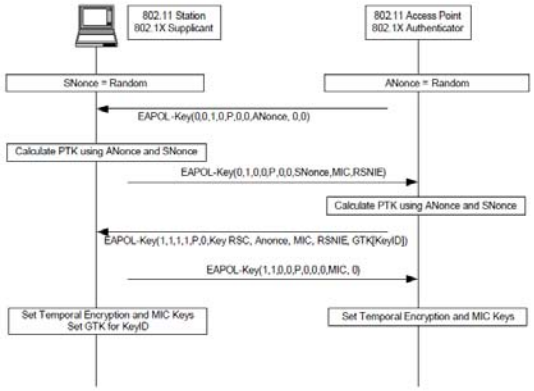



Figure 1: A sample 4-way handshake of IEEE 802.1X between a Station (S) and the Access Point (A) [1].

specified by IEEE 802.11e is applicable. It allows 4 different Access Categories (AC) to be used in addition to the standard Distributed Coordination Function (DCF), indicating the level of priority for a frame. A recent amendment specifies the prioritization of management frames [2]. It describes the quality of the service management frame (QMF) service, and is applicable to stations that provide QoS support. A station provides a QMF policy, which allows that station to selectively transmit management frames in other access categories than the one assigned to voice traffic (AC_VO). This shall improve the quality of service of other traffic streams. In any case, a station will use access category AC_VO for transmission to stations that do not support the QMF service.

### 2.2.2 TV-HORS

The multicast authentication scheme based on TV-HORS [11] is a v-time signature scheme. It extends on One-Time Signatures (OTS), to avoid excessive public key distribution, while providing tolerance to packet loss and being robust against malicious attacks. TV-HORS is a unidirectional scheme; to be used by 2 nodes to authenticate each other's traffic, it has to be applied by both nodes separately. A drawback of this scheme is its distribution of comparably large public keys varying between 8 to 10KB [11] as part of occurring initialization phases.

In the generic Time Valid-OTS scheme, a sender predefines and announces a signature period, with its private/public key assigned to this period. Messages sent within that period are then signed and verified using that key pair. With TV-HORS, one-way hash chains are used to link multiple key pairs together, with each only valid for a specific period of time. This time is referred to as epoch, effectively dividing a transmission session into epochs $P$. Each epoch is assigned a key pair. A parameter $v$ specifies the maximum number of packets that can be signed in each epoch. The scheme construction requires determining $T_\Delta$, the duration of an epoch $P$. Hence, a transmission session is bounded by $T_\Delta P$. A salt chain $k_j$ is constructed, and based on that, light chains are created. The elements $s_i$ of those light chains are referred to as Signature Authentic Generation Element (SAGE). For each new transmission session, a sender has to send initialization information to its receivers.

Table 2: Properties of TV-HORS and TRC

| Property | TV-HORS | TRC |
|---|---|---|
| WCET | no | yes |
| Reliability for msg delivery | no | yes |
| Broadcast | yes | yes |
| Multicast | yes | yes |
| Unicast | yes | yes |
| Integrity | yes | CRC |
| Authenticity | yes | no |

*Combining Properties.* Table 2 summarizes the individual safety and security properties of TV-HORS and TRC. Here, *integrity* is for TV-HORS the ability to detect intentional modification, but a weak property for TRC, detecting only unintentional/accidental modifications using CRC.

Looking at the protocols in isolation, one could either conduct 1) a dedicated analysis of TV-HORS with respect to satisfying properties for real-time communication, or 2) establishing claims about the TRC protocol executing in concordance to communication technology-dependent authentication mechanisms. Both of these approaches would either require strong assumptions on the underlying communication primitives in term of reliability and timeliness, or lead to rather qualitative results. Taking advantage of the case where security supports safety, we can by a straightforward modification embed TV-HORS in the real-time protocol. The TV-HORS signature for a packet is applied to any packet sent by the TRC protocol. This is done by both the TRC coordinator as well as the TRC node set. The TV-HORS initialization information for a new transmission session is also distributed as part of a TRC message. To preserve a deterministic packet size, a fixed amount of the application service data unit of a packet is reserved, to hold (part of) the initialization information. Therefore, sending the initialization information is treated as any other safety-critical message. Further, the same message resilience degree applies as for safety-critical messages, as well as the WCET guarantee. Drawback is the static overhead of the reserved buffer per message.

A coordinator in the AP receiving a part of a node's initialization information will publish that information to the backbone infrastructure. That way, subsequent APs the node is communicating with can use it in the new transmission session. Based on our use-case scenario, we can exploit the architecture properties of the communication system. For the purpose of this paper, we assume a fast and reliable wired AP backbone, to allow efficient replication of the initialization information to subsequent track-side APs.

Summarizing, embedding TV-HORS as part of the regular TRC message exchange a) decreases the size of the Application Service Data Unit (ASDU) due to TV-HORS data overhead, b) enforces the real-time protocol message schedule upon TV-HORS, and c) requires only IEEE 802.11 association for node handover.

Table 3: Communication Parameters and Simulation Settings

| Parameter | Setting | Description |
|---|---|---|
| Slot size | 15 ms | The slot size allocated by the real-time protocol to a single node per round |
| Protocol nodes | 5 | Real-time protocol nodes per AP |
| Interfering nodes | 8 total, 2 per AP | Compete for channel access, with traffic simulating saturation throughput |
| AP distance | 200 m | Distance between 2 APs |
| IEEE 802.11b DCF | 2 Mbit/s DQPSK | Robust coding scheme, and good reception at longer distances |
| Simulation Runs | 240 | Sequence of independent trials of the simulation |

# 3. ANALYSIS

Using the real-time protocol and authentication mechanisms described in Section 2, this section shows exemplary results of applying a set of metrics to the combined communication model, and further compare the real-time and authentication trade-off from a stochastic network simulation perspective. Of particular interest is the high cross-traffic scenario (close to saturation throughput), and single link setup. We neglect processing times for, e.g., frame processing, cyclic redundancy checks (CRC), and hash calculation. Experimental measurements and validation exist for the TRC protocol [7], and used for parametrization (see Table 3). We include the following results: the first part shows node handover with authentication to the AP based on WPA2. The algorithms for creating and using a RSNA are specified in IEEE 802.11. The essential part required for any of the four possible ways to use an RSNA is to establish temporal keys by executing a key management algorithm. During handover, service interruptions on that particular link for TRC protocol execution occurs, and allocated protocol slots for a node might be lost.

The second part shows the impact of TV-HORS exchanging its initialization information for subsequent authentication. The last part shows the trade-off for application-layer goodput based on the selected parametrization for moving train at different speeds.

## 3.1 Simulation Setup

For safety-critical tasks and strict real-time requirements, stochastic simulation and measurement-based approaches can aid support to formal analyses for e.g., temporal bounds as WCETs or bounds on resource allocation. A communication stack implementing the specification according to IEEE 802.11 offers a wide range of parameterization. Using an analytical model can usually not capture the whole parameter space, but limits itself to a small subset thereof. Here, modelling an evaluation setup in a network simulation environment has the advantage of a more thorough approximation to the specification. It provides first-hand evaluation possibilities of protocol modifications, with an insight on expected performance and the tightness of bounds as derived using e.g., analytical WCET tools. Simulation models further offer the possibility to conduct repeatable experiments for protocol modifications and altered parameter settings in the exact same environment conditions. This is very difficult with experimental measurements in a field setup. Network simulation models allow for generating detailed results for further evaluation of communication networks. A common characteristic is the observation of long tails in delays. From a safety perspective, we are frequently interested in the tails of delay distributions and the corresponding small probabilities (rare events), which are difficult to directly obtain. For that purpose, we can fit the delay curves from experiments to long tail distributions. It is one probabilistic approach for quantifying a safety-security trade-off. For our results, we chose a Pareto distribution as good fit for the delay tails.

The mobility model is created with respect to one moving node describing a train. The node moves along a given path resembling a railway track with constant speed. The access points are stationary at a-priori known positions along the railway track. The interfering stations serve for the purpose of saturating the channel along the path of the mobile node, and therefore approximate a highly contended link with concurrent access to the channel resources. From a practical point of view, such cross-traffic could occur—whether intentional or unintentional—on train station platforms or by passenger equipment on a train. See Figure 2 for a graphical description of the simulated layout in its initial state, and Table 3 for details on parameterization.

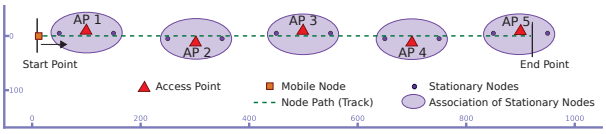



Figure 2: Map of stationary APs (triangles), initial locations of interfering nodes, and path of the mobile node.

## 3.2 WPA2

Figure 3 shows the delay contribution of the first 400 ms of the 4-Way handshake for creating and sharing the pairwise and group transient keys between the selected AP and the mobile node. Comparing the access categories underlines the possible negative impact of low QoS management frame settings on the handshake. This has an adverse effect on the real-time protocol schedule, indicating that frame prioritization of protocol and management frames should be aligned (preferably using AC_VO). Because the handover procedure is executed independently of the real-time protocol's slotting schedule, we are specifically interested in the effect on protocol time slots. Handover causes interruption of communication services by taking up a number of consecutive protocol time slots. Figures 4a and 4b show the consecutive loss for a node. That loss negatively impacts the message resilience degree, as lost slots are not applicable for message retransmission. One is the decrease in resilience of message requests (missed poll), the other message reception from other nodes (missed broadcast). As expected, the consecutive loss of Figure 4b is higher due to the AC_BK frame type. Applied as

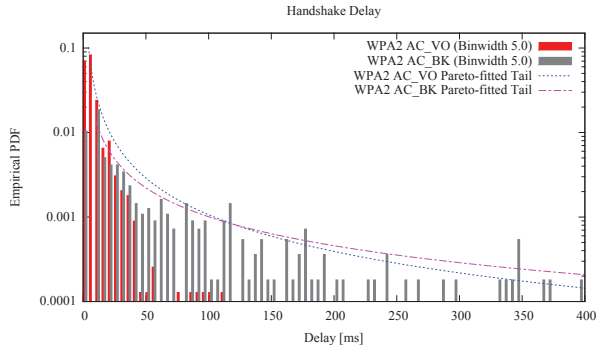


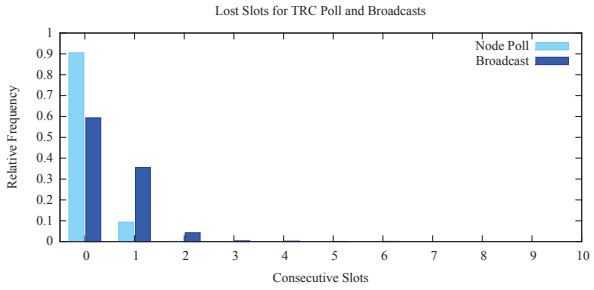

Figure 3: 4-way handshake delay contribution showing delays $\leq$ 400 ms in contended channel environment.

Table 4: TV-HORS Settings

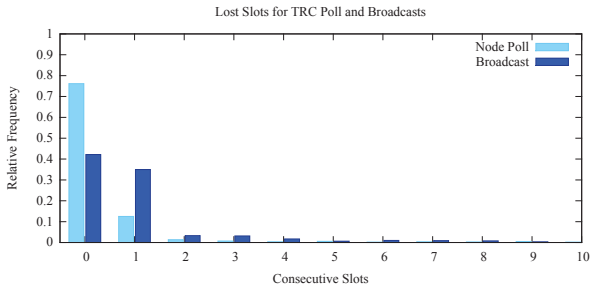
| Parameter | Setting | Description |
|---|---|---|
| Salt Chain Element $k_j$ | 80 Bits | The size of 1 salt chain element |
| SAGE $s_i$ | 48 Bits | The size of 1 light chain element |
| $v$ | 9 | Max. Numbers of packets signed in one epoch |
| $N$ | 1584 | The total number of SAGE chains |
| $t$ | 11 | Number of SAGEs contained in a message signature |
| Tx Session | 3600 s | The duration of a transmission session |

metric for protocol configuration, consecutive slot loss improves in addition to using other metrics, e.g., on-off loss models, including authentication for enhancing robustness. The results are based on the same experiments as Figure 3. Using those results for service disruption, the impact on a scheduled message can be modeled, e.g., violation of the required slots according to the message resilience degree.

Initiating the 4-way handshake can be improved by aligning it to the TRC protocol schedule. In defining a broadcast set $S_{bc}$, strictly the sender $s$ is part of $S_{bc}$, $s \in S_{bc}$ for message delivery. This can usually be relaxed, as $s$ does not have to receive its own broadcasted message. Therefore, for $s$ to not miss its own slot due to handover, a handover should take place after $s$ finished its outgoing messaging with the coordinator in its assigned slot. Broadcasts of subsequently scheduled nodes might be missed, but the time of all remaining slots $\{S_{bc} - s\}$ is available to complete the handover, sacrificing the own time slot with the least probability. Scheduling the handover that way, i.e., authentication and association, requires slight modification on the station trigger mechanism for handover initiation. It involves storing the decision obtained after the latest station probe request timeout. That decision is executed on finishing the sender's slot, i.e., after sending its request message to the coordinator.




(a) WPA2 using access category voice (AC_VO)




(b) WPA2 using access category background (AC_BK)

Figure 4: Lost node slots caused by WPA2 handover, distinguished by lost TRC poll and broadcast packets. Slot loss is a negative impact on the TRC message resilience degree.

## 3.3 TV-HORS

In contrast to the results shown for WPA2, no additional handshake is necessary with TV-HORS. A handover simplifies to a node association to the selected AP. Figure 5 shows the delays for association only.

Applying the parameterization as shown in Table 4, a communication overhead of 80 Bytes is required per message to carry the required scheme information. It can be calculated as $|s_i|t + |k_j| + |a| + |c|$ (see also Section 2.2.2). The variable $c$ denotes the current epoch, and $a$ refers to the $a^{th}$ message to be sent in that epoch. This overhead directly impacts the available size of the application service data unit for a sender. As described for the TV-HORS scheme, every new transmission session requires in advance the exchange of commitment values between a sender and receiver, the initialization information. The size of this initialization information distributed by the sender consist of $\langle k_0, Ns_i, T_\Delta, t_0^S, P \rangle$. The variable $t_0^S$ holds a timestamp referring to the beginning of the signature period, and is assumed to be 8 Bytes long. The information size required to be transmitted to a receiver (based on Table 4), is calculated allocating 9526 Bytes. Of interest in the trade-off analysis is the impact of transmitting that initialization information, also containing the sender's generated key. This initialization information is distributed as part of the executing real-time protocol. This is important, because the

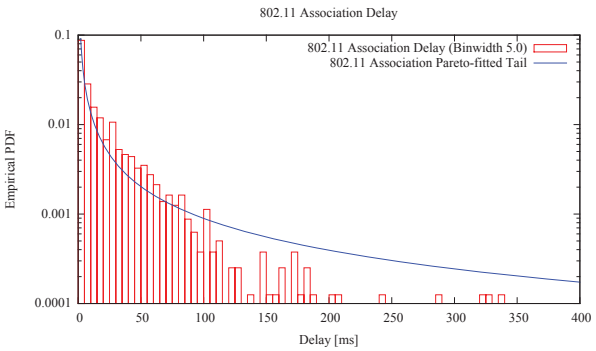



Figure 5: Node association time delay with Pareto-fitted tail.

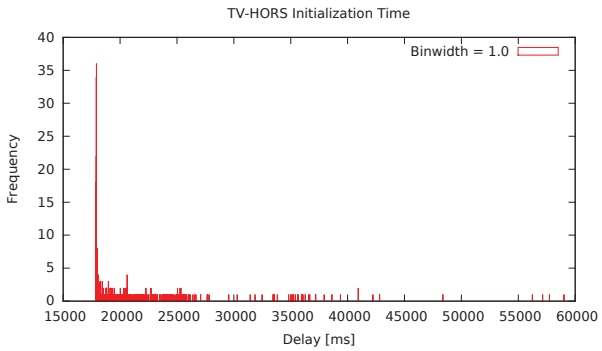



Figure 6: Transmission delay until TV-HORS initialization information is complete at the receiver.

same message resilience degree applies as for the distributed safety-critical messages.

Taking a typical maximum message of 200 Bytes, and accounting 80 Bytes for the signature, we permit additional 20 Bytes to transmit part of the generated initialization information, leaving a remaining size of 80 Bytes to the application. The result in Figure 6 shows the transmission delays for the initialization information for TV-HORS to receivers, until the complete information was received.

## 3.4 Application-layer Goodput

One metric from application-layer perspective is the impact of authentication on the TRC protocol, and in consequence, on the number of messages that are transmitted. For a fair comparison in terms of packet size, we configure the setup to always use the same ASDU length, taking into account the size of the MIC (8 Bytes) and the TV-HORS signature data. This allows the same assumptions on packet loss probability caused by bit errors. But it leads to a deterministic decrease in application-layer data for TV-HORS due to its bigger signature. An alternative approach would be to explicitly account for different packet sizes in the setup.

As discussed in Section 2.1, the TRC protocol uses a slotted, round-based schedule. The results in Figure 7 show the number of usable slots between handover for a moving node. This number depends on the associated times per AP at different speeds, one factor influencing goodput. We introduce $P_{HO}$ as the probability that handover completed within the timing bounds of the real-time protocol. Using $P_{HO}$, the protocol's WCET is configured to guarantee at least one node slot for transmission. Therefore, $P_{HO}$ is a measure for robustness during handover. Based on that, Figure 8 shows the expected application-layer goodput from the TRC protocol for different train speeds. We use $P_{HO} = 0.95$ and $P_{HO} = 0.99$ of the Pareto curve fit. For $P_{HO} = 0.99$, WPA2 with best-effort frames is omitted because the excessive handover delay incurs an unreasonable WCET. The histogram of Figure 4b and its high consecutive slot loss also shows the reason of that outcome. For example, taking a message resilience degree of 10 to configure the protocol, we would get a maximum detection time for node disconnect of $(\text{slot} * \text{nodes} * 10 + \text{slot}) = 765$ ms, using Table 3. The

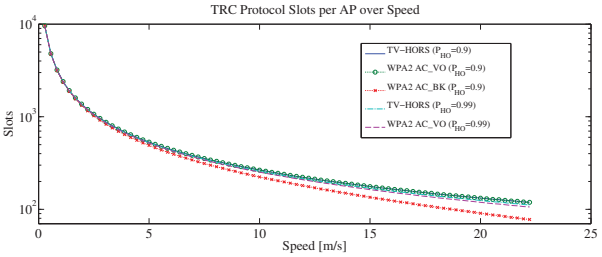



Figure 7: TRC protocol slots (in average) per AP.

probability that a handover is not completed at that point is $\approx 0.0072$ for AC_VO, but still $\approx 0.174$ for AC_BK. To gap those long delays, a higher resilience degree and/or longer slots are necessary.

While TV-HORS comes with the initial disadvantage of lower goodput (caused by the additionally transmitted signature), the additional impact by increasing speed is the lowest. In addition, it has the lowest increase in handover delays for $P_{HO}$ with ($P_{HO} > 0.99$). The goodput is calculated based on applicable slots per associated AP, and using the averaged simulation result for packet retransmission by the TRC protocol. That gives the application-layer goodput for executing the TRC protocol for message exchange.

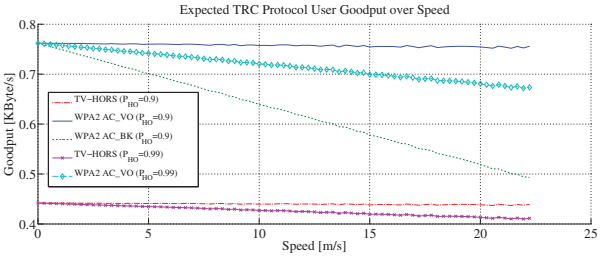



Figure 8: Impact of handover (association only, or with authentication) on TRC protocol goodput.

# 4. CONCLUSION

A methodology for combining safety and security properties might apply an analytical approach, where communication is formalized solely on deterministic initial conditions, variables are bounded, and communication behavior is modeled following cause and effect. With distributed systems using wireless networks and deploying standardized communication technologies and COTS components, the underlying techniques, e.g., CSMA/CA with backoff, and characteristics of communication networks, e.g., long tails in communication delays, add considerable complexity and uncertainty to such approaches. In such cases, a quantification based on a probabilistic modeling can aid in analyzing the trade-offs in safety and security. A parametrization using stochastic methods and discrete event network simulations can provide a useful starting point for further analysis.

For our analysis, we extend on previous work by quantifiying trade-offs for communication aspects when facing both safety and security requirements in the design of safety-critical systems. We use a real-time protocol for the distribution of safety-critical messages to assess required procedures in node handover. Besides the standard WPA2 4-way handshake, we include the efficient one-time signature multicast authentication scheme TV-HORS. By embedding TV-HORS into the real-time protocol, both the safety and security properties apply. We establish metrics to evaluate where security has a negative impact on safety. Metrics include handover and authentication delays, missed node slots in the protocol schedule, and application-layer goodput for real-time messaging. The real-time protocol's slot metric is an important configuration factor in parameterization for channel contention, with direct influence on message resilience degree and protocol WCET. Authentication during handover impacts the number of slot misses, the WCET affects distributing TV-HORS initialization information. TV-HORS simplifies node handover, with the AP directly verifying signatures. This leads to a more efficient and robust handover; the downside is transmission of large initialization information for each new transmission session. For deterministic packet sizes, this considerably affects the maximum size of the application service data unit.

Understanding the merits of different mechanisms provides one step in the convergence of joint modeling safety and security. A combined quantification aids in establishing more complex probabilistic models. We can focus on communication specifics and the deployed communication technology, to quantitatively compare selected metrics as measure for throughput, loss, and delay. Our setup resembles part of a metropolitan railway communication architecture deploying IEEE 802.11. Using ns-3 to prototype the communication and authentication protocols, we implemented the metrics of choice in the simulation models. Both the real-time protocol and TV-HORS are not limited to IEEE 802.11, and the addressed problem also applies to other communication technologies with authentication requirements, not necessarily during handover. The overall evaluation focus of quantifying service degradation or disruption caused by security measures is extensible to e.g., backbone links, or authentication of intelligent electronic devices in smart grids.

Future work will address the adaptation for other real-time protocols, the combination with different mobile support architecture, e.g., Mobile IP, detailed quantification of security levels to optimize the safety-security trade-off, and continuing the integration in design approaches on a system level.

# 5. ACKNOWLEDGMENTS

This work has been performed within ARTEMIS SESAMO (grant no. 295354). FTW is supported by the Austrian Government and by the City of Vienna within the competence center program COMET.

# 6. REFERENCES

[1] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-2007*, June 2007.

[2] Prioritization of management frames. *ISO/IEC/IEEE 8802-11:2012/Amd.1:2014(E)*, Mar. 2014.

[3] Artemis SESAMO. SEcurity and SAfety MOdelling, Technical Annex, Feb. 2012.

[4] R. Bloomfield, K. Netkachova, and R. Stroud. Security-informed safety: If it's not secure, it's not safe. In *Software Engineering for Resilient Systems*, volume 8166 of *Lecture Notes in Computer Science*, pages 17–32. Springer Berlin Heidelberg, 2013.

[5] S.-M. Chang, S. Shieh, W. W. Lin, and C.-M. Hsieh. An efficient broadcast authentication scheme in wireless sensor networks. In *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '06, pages 311–320, NY, USA, 2006. ACM.

[6] F. Flammini, S. Marrone, M. Iacono, N. Mazzocca, and V. Vittorini. A multiformalism modular approach to ERTMS/ETCS failure modelling. *International Journal of Reliability, Quality and Safety Engineering*, 21(01):1450001–1–1450001–29, 2014.

[7] B. Malinowsky, J. Gronbaek, H.-P. Schwefel, A. Ceccarelli, A. Bondavalli, and E. Nett. Timed broadcast via off-the-shelf WLAN distributed coordination function for safety-critical systems. In *Dependable Computing Conference (EDCC), 2012 Ninth European*, pages 144–155, May 2012.

[8] D. Nicol, W. Sanders, and K. Trivedi. Model-based evaluation: from dependability to security. *Dependable and Secure Computing, IEEE Trans. on*, 1(1):48–65, Jan 2004.

[9] L. Pièvre-Cambacédès and M. Bouissou. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). In *Systems Man and Cybernetics (SMC), 2010 IEEE International Conf. on*, pages 2852–2861, Oct 2010.

[10] J. Smith, S. Russell, and M. Looi. Security as a safety issue in rail communications. In *Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software - Volume 33*, SCS '03, pages 79–88, Darlinghurst, Australia, 2003.

[11] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt. Time valid one-time signature for time-critical multicast data authentication. In *INFOCOM 2009, IEEE*, pages 1233–1241, Apr. 2009.