Security-aware Signal Packing Algorithm for CAN-based Automotive Cyber-physical Systems

Yong Xie, *Member, IEEE*, Liangjiao Liu, Renfa Li, *Senior Member, IEEE*,
Jianqiang Hu, Yong Han, and Xin Peng

***Abstract*—Network and software integration pose severe challenges in cyber-security for controller area network (CAN)-based automotive cyber-physical system (ACPS), therefore we employ message authentication code (MAC) to defend CAN against masquerade attack, but the consequent bandwidth overhead makes it a necessity to find the tradeoff among security, real-time and bandwidth utilization for signal packing problem (SPP) of CAN. A mixed-security signal model is firstly proposed to formally describe the properties and requirements on security and real-time for signals, and then a mixed-integer linear programming (MILP) formulation of SPP security-aware signal packing (SASP) is implemented to solve the tradeoff problem, where the bandwidth utilization is improved and the requirements in both security and real-time are met. Experiments based on both society of automotive engineers (SAE) standard signal set and simulated signal set showed the effectiveness of SASP by comparing with the state-of-the-art algorithm.**

***Index Terms*—Signal packing, security, automotive cyber-physical systems (ACPS), integer linear programming.**

I. Introduction

As many societal and economical requirements are put on automobiles, such as the improvement of driving performance and comfort, and the enhancement of both passive and active safety, more and more information and communication technology (ICT) contents are brought into the automotive electronic systems in the forms of software, network, and etc[1]. As a result, automotive electronic systems are evolved from a close system to an open automotive cyber-physical system (ACPS) comprising of 70 to 100 electronic control units (ECUs) interconnected by several networks[2−3].The openness of ACPS brings many new exciting experiences to the automobile users, while at the same time it imposes severe challenges in cyber-security to auto industry[4−5]. In [6−7], the authors showed that ACPS could be attacked through various interfaces, including direct and indirect physical access, short-range and long-range wireless channels. Cyber-security problems produce numerous adverse impacts to the driver, varying from the discomfort caused by malfunction of air conditioner to endangering of driver and passenger's life. Despite of these potential cyber-security vulnerabilities, functions of different criticalities (like safety-critical, function-critical and non-critical functions) are integrated into the same ECU in ACPS because of the pressure from size, weight, and power (SWaP) properties[2]. As a consequence, the cyber-security threat is daily increasing for ACPS.

Controller area network (CAN) is the most widely employed real-time communication technologies in ACPS[8], However, it is designed without the consideration of cyber-security. And in itself there are several cyber-security vulnerabilities[5], such as CAN is a CSMA/CD protocol and CAN messages are being broadcasted to all ECU nodes on the network, which means that attacker can easily eavesdrop on the network and read the content of the messages; CAN message do not contain any information to authenticate its sender, thus attacker can potentially masquerade other ECU and send the messages, and etc. Due to the above vulnerabilities, CAN becomes the ideal attacking object for cyber-security attackers in ACPS[9−13]. Taking the wide application of CAN in auto industry into account, huge price needs to be paid if the existing CAN specification is modified to protect it against the cyber security attackers. Therefore, the feasible security mechanism should be designed to be compatible with the current CAN specification. In this paper, the MAC-based security enhancement mechanism is integrated into the signal packing problem (SPP) of CAN[14−18], but the bandwidth overhead brought together makes it a necessity to find the tradeoff among the cyber-security, real-time and bandwidth utilization, as CAN's bandwidth is limited to 1 Mbps, and CAN message's maximal payload is limited to 8 bytes.

After the above analysis, we can find that SPP is a typical multi-objective optimization problem. In this paper, we set the requirement in cyber-security and real-time as the key constraints, because only as far as the requirements on these two non-functional properties are met, system's safety can be guaranteed. We set bandwidth utilization as the final optimization objective due to the limitation of CAN's bandwidth. Through this research, a security-aware signal packing (SASP) algorithm is proposed for CAN, and the minimization about the bandwidth's overhead brought by security enhancement

Manuscript received September 2, 2014; accepted August 9, 2015. This work was supported by National Natural Science Foundation of China (61502405, 61300039), Provincial Science Foundation of Hunan Province (14JJ3130), Fujian Educational Bureau (JA15368), and Xiamen University of Technology (YKJ13024R, XYK201437). Recommended by Associate Editor Yilin Mo.

Citation: Yong Xie, Liangjiao Liu, Renfa Li, Jianqiang Hu, Yong Han, Xin Peng. Security-aware signal packing algorithm for CAN-based automotive cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, 2015, **2**(4): 422−430

Yong Xie, Jianqiang Hu, and Yong Han are with the Key Laboratory for Application Technology of Internet of Things of Fujian Educational Bureau, Xiamen University of Technology, Xiamen 361024, China (email: yongxie@xmut.edu.cn; jqhucn@xmut.edu.cn; yonghan@xmut.edu.cn).

Liangjiao Liu and Renfa Li are with the Key Laboratory of Embedded and Networking Computing of Hunan Province, Hunan University, Changsha 410082, China (email: lirenfa@vip.sina.com; llj1984109@qq.com).

Xin Peng is with the Key Laboratory on Complex Systems Optimization & Controlling of Hunan High Education Institutions, Hunan Institute of Science and Technology, Yueyang 414000, China (email: peng-xin@foxmail.com).

is pursued to improve the bandwidth utilization of CAN and consequently to lower the cost for ACPS.

II. Related work

A. Related Work About the SPP of CAN

SPP can be seen as a special case of the bin packing problem, which is known to be a NP-hard optimization problem. There are several works addressing the SPP with heuristics, and bandwidth utilization and message's schedulability are the general optimization objective. Sandstrom et al.[14] propose a next-fit-decreasing based heuristic packing algorithm to optimize the bandwidth utilization. Polzlbauer et al.[15] define a metric of bandwidth utilization, and based on it a packing algorithm is designed to optimize both bandwidth utilization and message's schedulability. And later, Polzlbauer et al.[16] present another extensibility-aware packing algorithm, which is based on the simulated annealing and the bandwidth utilization is its optimization objective.

Some other research tries to combine the SPP with message scheduling, which are the two key design problems of CAN. Saket et al.[17] propose a best-fit-decreasing based heuristic to optimize the bandwidth utilization with deadline constraint. Pop et al.[18] use the offset to order the signals, and a heuristic algorithm is given to improve message's schedulability. Zheng et al.[19]and Zhu et al.[20] integrate the design of CAN and ECU into the same optimization framework, and their objectives are end-to-end WCRT (Worst-case response time) and extensibility, respectively. However, cyber-security is not considered in the above works, while our work tries to find the balance among cyber-security, real-time and bandwidth utilization for SPP.

B. Related Work About the Security Enhancement Mechanisms of CAN

MAC-based authentication is a widely used security enhancement mechanism for CAN. Nilsson et al.[10] raise a message authentication method with the compound MAC, which supports the split and assembly of MAC and can protect CAN from injection attack and tempering attack. Groza et al.[11] give a light broadcasting authentication mechanism for CAN, which supports the MAC sharing among different nodes and the separate transmitting of MAC and message. Van Herrewege et al.[12] propose a MAC-based backward compatible broadcast authentication protocol for CAN+. Han et al.[13] combine the MAC-based authentication with the anonymous ID based message filtering to defend the CAN against injection and modification attack. However, the above works focus only on the security enhancement mechanisms, while our work integrates the security consideration into the multi-objective design optimization problem of CAN.

Lin et al. add both the MAC and counter into the CAN message to protect it from masquerade attack and replay attack, and then they also integrate the security mechanism into the design process of CAN in [21]. This latest work integrates the SPP of CAN and task allocation together, and a grouping mechanism is used to decrease the bandwidth overhead brought by the security mechanism, its optimization objective is the end-to-end WCRT. The difference between Lin et al's work and our work is in two aspects:

1) Lin et al. assume the same security requirement for all signals, while our work takes the software integration trend of ECUs into account and considers the different levels of security requirements for signals included in functions of different criticalities.

2) We set the bandwidth utilization as the optimization objective and treat the real-time requirement only as a constraint. As for CAN, only if the deadline is not violated for message, system's safety can be guaranteed, no matter what is the specific WCRT of message. While its bandwidth is quite limited, thus the bandwidth utilization should be improved as much as possible.

After the above analysis, we can come to the conclusion about the shortcomings of the related works:

1) Security is not considered enough in the design of CAN system, and the tradeoff among the security, real-time and bandwidth utilization is still an open question;

2) Different levels of security requirement for mixed criticality functions included in the same ECU is out of their consideration, which will cause the over-design of ACPS.

Aiming at compensating for the above shortcomings, we first give a mixed security signal model to formally describe the properties and requirement in security and real-time for signals included in mixed criticality functions. Based on that, an optimal MILP formulation based SASP is proposed for SPP to find the tradeoff among security, real-time and bandwidth utilization, where the bandwidth utilization is improved and the requirements on security and real-time are both met.

III. System model and assumptions

A. Signal Model and Message Model

As shown in Fig. 1, this is a typical CAN-based ACPS. ECU set is indicated as: $ECU = \{E_1, E_2, \ldots, E_k, \ldots, E_N\}$. There is a signal set in ECU E_k and it is indicated as: $S_k = \{s_{k,1}, s_{k,2}, \ldots, s_{k,i}, \ldots, s_{k,L}\}$, where $L \in \mathbf{N}^+$ and L represents the number of signals in S_k. As the signal packing is only used for signals belonging to the same ECU, we omit the subscript k of signal's notation to keep the signal model clear and simple, thus s_i is used to indicate the signal for the following part of this paper, and $s\_own(i, k)$ is used to indicate the relation between s_i and E_k. Real-time properties of signal can be described with a 3-tuple, s_i:$\{s\_period(i), s\_size(i), s\_deadline(i)\}$, which indicates the period, transmission time and deadline of s_i, respectively, and we assume that the deadline equals to the period for all signals and messages.

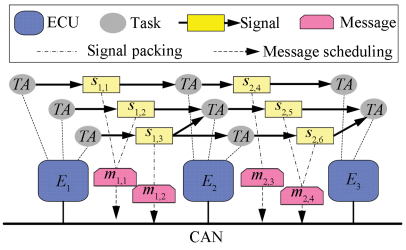


Fig. 1. CAN-based automotive cyber-physical system.

Signals in S_k need to be packed into messages before they can be transmitted on CAN, and how many messages will be generated depends on the used packing algorithm. The obtained message set in E_k is represented as $M_k = \{m_{k,1}, m_{k,2}, \ldots, m_{k,i}, \ldots, m_{k,L'}\}$where $L' \in \mathbf{N}^+$ and $L' \leq L$. As shown in Fig.1, the signal set contained in E_1 is: $S_1 = \{s_{1,1}, s_{1,2}, s_{1,3}\}$, and the corresponding message set is: $M_1 = \{m_{1,1}, m_{1,2}\}$, where $m_{1,1} = \{s_{1,1}, s_{1,2}\}$, $m_{1,2} = \{s_{1,3}\}$. For the same reason described before, we also omit the subscript k of message's notation for the following part of this paper, and use $m\_own(j,\ k)$ to describe the belonging ECU of m_j. Real-time properties of m_j can be described with a 3-tuple: $\{m\_period(j),\ m\_size(j),\ m\_deadline(j)\}$, which indicate the period, transmission time and deadline of m_j, respectively. If signals with different periods are packed into the same message, there will be oversampling for signals with relatively bigger period. As a consequence, we assume that only the signals with the same period can be packed into the same message, which is a common assumption in other works such as [15−16, 21−22]. Period, transmission time and deadline of m_j can be calculated with the following equations:

$$m\_period(j) = s\_period(i), s_i \in m_j, \tag{1}$$

$$m\_size(j) = \sum_{s_i \in m_j} s\_size(i), \tag{2}$$

$$m\_deadline(j) = s\_deadline(i), s_i \in m_j. \tag{3}$$

We assume that signals are packed according to the standard format of CAN, thus *m_size*(j) can be calculated from (4)[23]:

$$\text{m\_size}(j) = (55 + 10 \cdot PL_j) \cdot \tau_{bit}, \tag{4}$$

where PL_j indicates the payload of m_j, and τ_{bit} indicates the time for CAN to transmit 1 byte. We assume the bandwidth of CAN is 500 kbps. The payload of CAN message varies from 1 bit to 8 bytes, and besides it there are other segments in message such as the ID and CRC, which are the cause of the bandwidth overhead in message itself. According to (4), the bandwidth overhead for CAN message can vary from 41.35 % to 97.8 %.

B. Attacker Model and Security Mechanism

The masquerade attack is potentially one of the most popular attacking approach on CAN[5, 21−22], thus we mainly try to defend the CAN from the masquerade attack in this paper, and the MAC-based authentication mechanism is employed[10−13, 21−22]. According to this mechanism, there is a public key shared between any two communicating ECUs. The message sender uses the key and the content of the message to generate a MAC MAC_s, and MAC_s is also packed into the message together with the signals. After the message's transmission, another MAC MAC_r will be generated in the receiver node according to the content of the received message and the shared key, and a comparison between the MAC_s and MAC_r is done to authenticate the identity of the message sender and make sure that the content of the message is not modified by any other attacker. When the signals inside the same message have the same receiving ECU, they can share the same MAC to reduce the bandwidth overhead. And when there are different receiving ECUs for the same message, several MACs need to be generated and added into the message.

The security mechnism adopted in this paper is MAC-based, if the attacker does not have any prior knowledge about the MAC, guess of the MAC is quite random, and the success probability of the masquerade attack is 2^{-H}, where H indicates the length of MAC (in bits). On the contrary, if we know the security requirement of the functions, (5) can be used to calculate the value of H, where P represents the security requirement put on message.

$$H = \log_2 \frac{1}{P}. \tag{5}$$

C. Mixed Security Signal Model

The pressure from the SWaP property will gradually transform the ACPS into a mixed-criticality system, where several functions with different criticalities are integrated into the same ECU[2]. The functional safety standard ISO 26262[24] is proposed to give formal and quantitative description about the safety requirement (such as the dependability, security and etc) for automobiles, where the functions are classified into four categories with different levels of safety requirement (or criticality). Therefore, different levels of security protection are needed for signals included in functions with different criticality. In this paper, we extend the basic signal model described in Section III-A and propose a mixed-security signal model to formally describe the security requirement on signals.

We divide the functions in ACPS into two categories: Fun_{HI} and Fun_{LO}, which have the high and low level of security requirement, respectively. The mixed-security signal model used to describe the signals with mixed-level of security requirements is described as s_i: $\{s\_period(i),\ s\_size(i),\ s\_deadline(i),\ s\_mac(i)\}$, and $s\_mac(i)$ indicates the length of MAC needed to obtain the required level of security for s_i. For signals belonging to the functions with higher level of security requirement, their s_mac(i) is larger that that of the signals belonging to the functions with lower level of security requirement. We assume that the security requirement of the functions is known as in [21−22], so $s\_mac(i)$ can be calculated with (5). As far as we know the required security levels put on functions, this mixed-security signal model can be easily extended to describe the signals with more levels of security requirements.

IV. MILP FORMULATION OF THE PROPOSED SASP

SPP can be seen as a special case of the Bin Packing problem[14−16], where signals are the objects needed to be packed into the bins (messages). The size of bin equals to that of the message with maximal payload, and the number of bins equals to that of the signals. The difference is that signals may have different sizes, periods and different levels of security requirement, the packing rules need to be extended to further include the requirements on security and real-time, and the objective is changed to minimize the space utilization of bins (the sum of the bandwidth utilization of all messages).

MILP is a powerful method that is often used to solve the bin-packing problem, thus we also formulate the SPP problem into a MILP problem and solve it with the CPLEX tool developed by IBM.

In this section, we first give all the constraints needed to be met by SASP, and then the objective function is explained. Tables I and II show all the known variables and the unknown variables requiring to be solved. The value of binary variable is 1 if the condition is true and 0 otherwise.

A. Constraints

For all the following constraints, i and i' are the labels for signals, j and j' are the labels for messages, and k and k' are the labels for ECUs.

1) Constraint on mapping relation between signals and messages

$$\forall s_i \in S_k, k,$$
$$\sum_j assign(i,k,j) = s\_own(i,k) \times m\_own(j,k), \tag{6}$$
$$\forall s_i \in S_k, k, j, \quad assign(i,k,j) \le taken(k,j). \tag{7}$$

Equation (6) indicates the constraint that each signal is exactly packed into only one message, (7) indicates the condition that if signal s_i is packed into m_j of E_k, if that is the truth, then $taken\ (k,\ j) = 1$.

2) Constraint on size and period of messages

According to the security mechanism proposed in this paper, two different parts are contained in message's payload: signals and the attached MACs. Equation (8) calculates the payload for m_j, which equals to the sum size of the included signals. Equation (9) indicates the constraint that the maximal payload of message should not be overloaded. Equation (10) calculates the transmission time of m_j.

$$\forall m_j \in M_k, k,$$
$$m\_size(j) = \sum_i assign(i,k,j) \times (m\_mac\_t(j) + s\_size(i)), \tag{8}$$

$$\forall m_j \in M_k, k,$$
$$\sum_i assign(i,k,j) \times \frac{m\_mac\_t(j) + s\_size(i)}{8} \le capacity, \tag{9}$$

$$\forall m_j, \quad m\_t\_size(j) = \frac{55 + 10 \times \frac{m\_size(j)}{8}}{speed}. \tag{10}$$

According to our assumption that only signals with equal periods can be packed into the same message, message's period equals to that of the included signals. Thus, (11) and

TABLE I
THE KNOWN VARIABLES IN THE MILP FORMULATION

Name	Type	Definition
$s\_own(i,\ k)$	Binary variable	If the belonging ECU of s_i is E_k
$m\_own(j,\ k)$	Binary variable	If the belonging ECU of m_j is E_k
$sm(i,\ i')$	Binary variable	If the security requirements of s_i and $s_{i'}$ are the same
$s\_mac(i)$	Real variable	The length of MAC (in bits) needed to acquire the required level of security for s_i
$s\_size(i)$	Real variable	The size of s_i (in bits)
$s\_period(i)$	Real variable	The period of s_i (in ms)
$speed$	Real variable	The bandwidth of CAN (500 kbps)
$capacity$	Real variable	The maximal payload of CAN message (8 bytes)

TABLE II
THE UNKNOWN VARIABLES IN THE MILP FORMULATION

Name	Type	Definition
$assign(i,\ k,\ j)$	Binary variable	If s_i is packed into m_j in E_k
$taken(k,\ j)$	Binary variable	If m_j in E_k is occupied
$m\_mac\_t(j)$	Real variable	The length of MAC (in bits) needed to acquire the required level of security for m_j
$m\_mac(j)$	Real variable	The sum length of MAC (in bits) needed to acquire the required level of security for all signals in m_j
$m\_size(j)$	Real variable	The size of m_j (in bits)
$m\_t\_size(j)$	Real variable	The transmission time of m_j (in ms)
$m\_period(j)$	Real variable	The period of m_j (in ms)
$hp(j,\ j')$	Binary variable	If the priority of m_j is greater than that of $m_{j'}$
$block(j)$	Real variable	The blocking time for m_j (in ms)
$m\_r(j)$	Real variable	WCRT of m_j (in ms)
$s\_r(i)$	Real variable	WCRT of s_i (in ms)
W	Constant	A large constant for linearization

(12) are used to define the constraints about the period of signal and message.

$$\forall s_i \in S_k, k, j,$$
$$assign(i,k,j) \times s\_period(i) \leq m\_period(j), \quad (11)$$

$$\forall s_i \in S_k, k, j,$$
$$assign(i,k,j) \times m\_period(j) \leq s\_period(i). \quad (12)$$

3) Constraint on security

We consider about the signals with different levels of security requirement, and there are two possible packing strategies for them. Strategy 1 does not allow signals with different levels of security requirement to be packed into the same message, thus all the signals inside the same message have the same level of security requirement, and the security requirement of the message equals to that of the included signals. While Strategy 2 allows signals with different levels of security requirement to be packed into the same message, so we need to give all the included signals the high level of security protection, or else signals with relatively lower security requirement will become the weakness of the message, and the attacker can take advantage of them to attack the message successfully with lesser efforts. Consequently, message's security requirement is equal to the relatively higher security requirement of the included signals. Equation (13) indicates the required level of security for message:

$$\forall m_j \in M_k, k,$$
$$m\_mac\_t(j) = \max(assign(i,k,j) \times s\_mac(i)). \quad (13)$$

After the constraint on period defined in (11) and (12) that only signals with the same period can be packed into the same message, (14) is further used in strategy 1 to enforce the constraint that only signals with the same level of security requirement can be packed into the same message, where $sm(i,\ i')$ indicates if the security requirement on s_i and $s_{i'}$ are the same or not. As Strategy 2 allows signals with different levels of security requirement to be packed together, no constraint needs to be defined for it.

$$\forall s_i, s_{i'} \in S_k, k, j,$$
$$assign(i,k,j) + assign(i',k,j) + sm(i,i') \neq 2. \quad (14)$$

According to Strategy 1, signals with different levels of security requirement need to be divided into different messages even if their periods are the same, but those signals can be packed together originally when security is not considered. As a consequence, more messages will be generated in Strategy 1 comparing with Strategy 2, and it brings extra bandwidth overhead originated from the bandwidth overhead in message itself. However, although Strategy 2 allows more signals to be packed together, the length of MAC corresponding with the signals with relatively lower level of security requirement needs to be increased so as to guarantee the security of the obtained message. Consequently, Strategy 2 also causes extra bandwidth overhead. As the comparison experiment showed in Section V, Strategy 2 is better than Strategy 1 in bandwidth utilization, thus strategy 2 is used in SASP.

After the above analysis, the sum of MAC that is needed to obtain the required level of security for all signals included in m_j can be calculated according to (15):

$$\forall m_j \in M_k, k,$$
$$m\_mac(j) = \sum_i assign(i,k,j) \cdot m\_mac\_t(j). \quad (15)$$

4) Constraint on response time of message and signal

For constraint on response time of message, we first give the feasible priority assignment, and then the analysis about the blocking time and WCRT[22−23].

a) Priority assignment

As each CAN message has a unique priority, (16) and (17) are used to indicate the constraint on priority relation of any two messages. Equation (18) indicates the transitive property of the priority relation among messages. For example, if $hp(j,j')=1$ and $hp(j',j'')=1$, then $hp(j,j'')=1$.

$$\forall m_j,\ hp(j,j)=0, \quad (16)$$

$$\forall m_j, m_{j'}, k, j \neq j', \quad hp(j,j') + hp(j',j) = 1, \quad (17)$$

$$\forall m_j, m_{j'}, m_{j''}, k, j \neq j', j' \neq j'',$$
$$hp(j,j') + hp(j',j'') - 1 \leq hp(j,j''). \quad (18)$$

b) Blocking time analysis

As CAN messages are scheduled non-preemptively, $block(j)$ is used to indicate the blocking delay caused by other messages with lower priority for m_j, and it can be calculated with

$$\forall m_j, m_{j'}, k,\ block(j) = \max(m\_t\_size(j),$$
$$hp(j',j) \times m\_t\_size(j')). \quad (19)$$

c) Response time analysis for message

Equation (20) is used to analyze the WCRT for m_j, the first part indicates the experienced blocking time, the second part indicates the transmission time of m_j itself, and the third part indicates the preemption delay caused by other messages with higher priority. Equation (21) describes the schedulability constraint on message's response time:

$$\forall m_j, m_{j'}, k, \quad m\_r(j) = block(j) + m\_t\_size(j) + \sum_{j'} taken(k,j) \times hp(j',j) \times \left\lceil \frac{m\_r(j) - m\_t\_size(j)}{m\_period(j')} \right\rceil \times m\_t\_size(j'), \quad (20)$$

$$\forall m_j, m_{j'}, k, \quad block(j) + m\_t\_size(j) + \sum_{j'} taken(k,j) \times hp(j',j) \times \left\lceil \frac{m\_r(j) - m\_t\_size(j)}{m\_period(j')} \right\rceil \times m\_t\_size(j') \leq m\_period(j). \quad (21)$$

d) Response time analysis for signal

As Strategy 2 is used for SPP, signal's WCRT equals to that of the belonging message, so (22)-(23) defines the WCRT for signals. W is a big constant needed for linearization.

$$\forall s_i \in S_k, k, j, \quad m\_r(j) - W \times (1 - assign(i,k,j)) \leq s\_r(i), \tag{22}$$

$$\forall s_i \in S_k, k, j, \quad s\_r(i) \leq m\_r(j) + W \times (1 - assign(i,k,j)). \tag{23}$$

B. Objective Function

We set bandwidth utilization as the optimization objective of SASP, and it is calculated by summing up the consumed bandwidth of the occupied messages as described in (24), where the consumed bandwidth of each message is obtained by dividing its size by its period.

$$Objective : \forall m_j \in M_k, k, \quad \sum_j taken(k,j) \times \frac{m\_size(j)}{m\_period(j)}. \tag{24}$$

C. Conversion to Linear Constraints

For the described MILP formulation above, (14), (20), (21) and (24) are needed to be linearized before they can be solved by CPLEX tool[22]. Equation (14) is an inequality of summation of three binary variables, and it can be linearized and replaced with the following equations:

$$\forall s_i, s_{i'} \in S_k, k, j, \quad assign(i,k,j) + assign(i',k,j) - sm(i,i') \leq 1, \tag{25}$$

$$\forall s_i, s_{i'} \in S_k, k, j, \quad assign(i,k,j) - assign(i',k,j) + sm(i,i') \leq 1, \tag{26}$$

$$\forall s_i, s_{i'} \in S_k, k, j, \quad -assign(i,k,j) + assign(i\prime,k,j) + sm(i,i\prime) \leq 1. \tag{27}$$

Equations (20) and (21) can be linearized similarly in three steps. First, the ceiling function $\lceil x \rceil$ can be replaced by a non-integer variable y, and another constraint: $0 \leq y - x \leq 1$ is added. Second, the multiplication of two binary variables x and y can be replaced by a binary variable z, and then one constraint is added as: $x \times y = z$. And then $x \times y = z$ can be replaced by equivalent constraints: $x + y - 1 \leq z$, $z \leq x$ and $z \leq y$. Third, the multiplication of one binary variable x and one non-integer variable y can be replaced by a non-integer variable z, and one constraint $x \times y = z$ is added. Next, $x \times y = z$ can be replaced by equivalent constraints: $0 \leq z \leq y$ and $y - W \times (1 - x) \leq z \leq W \times x$. For example, (20) can be linearized and replaced with (28), and six more constraints described by (29) through (34) are added:

$$\forall m_j \in M_k, k, \; m\_r(j) = block(j) + m\_t\_size(j) + \sum_{j'} Z(j,j',k) \times m\_t\_size(j'), \tag{28}$$

$$\forall m_j, m_{j'}, \; 0 \leq X(j,j') - \frac{m\_r(j) - m\_t\_size(j)}{m\_period(j')} \leq 1, \tag{29}$$

$$\forall m_j, m_{j'}, k, \; 0 \leq taken(k,j) + hp(j',j) - 1 \leq Y(j,j',k), \tag{30}$$

$$\forall m_j, m_{j'}, k, \; Y(j,j',k) \leq taken(k,j), \tag{31}$$

$$\forall m_j, m_{j'}, k, \; Y(j,j',k) \leq hp(j',j), \tag{32}$$

$$\forall m_j, m_{j'}, k, \; 0 \leq Z(j,j',k) \leq Y(j,j',k), \tag{33}$$

$$\forall m_j, m_{j'}, k, \; Y(j,j',k) - W \times (1 - X(j,j')) \leq Z(j,j',k) \leq W \times X(j,j'). \tag{34}$$

Equation (24) also includes a multiplication of binary variable and one non-integer variable, and it can be linearized with the same approach as described above. Equation (24) can be replaced with (35) and two more constraints described by (36) and (37) are added:

$$\text{Objective} : \forall m_j, k, \; \sum_j Z(k,j), \tag{35}$$

$$\forall m_j, k, \; 0 \leq Z(k,j) \leq \frac{m\_size(j)}{m\_period(j)}, \tag{36}$$

$$\forall m_j, k, \; \frac{m\_size(j)}{m\_period(j)} - W \times (1 - taken(k,j)) \leq Z(k,j) \leq W \times taken(k,j). \tag{37}$$

V. Experimental analysis

Two sets of experiments based on signal sets from different sources are done to verify the effectiveness of the SASP by comparing it with the SPP algorithm proposed in [22]. The first signal set is a standard CAN signal set from the SAE[25], which represents the requirement from the industry. And the second one is generated by Netcarbench 3.4[26], which is a popular simulation tool for CAN Network. According to the ISO 26262, there are four levels of security requirement in ACPS, which are L_1-L_4, respectively, and we assume that the corresponding length of MACs are 2/4/6/8 (in bit). The MILP formulation of SASP is implemented in ILOG CPLEX Optimization Studio 12.6 from IBM, and the configuration of the PC running the experiments is: Intel(R) Core(TM)2 2.13 GHZ and 2 GB RAM.

A. Introduction About the Two Employed Signal Sets

1) SAE signal set

The SAE standard signal set is corresponding to a CAN network composed with 7 ECU nodes and 53 signals, signal's size varies from 1 bit to 8 bits, and signal's period varies from 5 ms to 1 000 ms, please refer to [25] for more details about this signal set. When security is not considered, the number of the obtained messages is 17 and the bandwidth utilization is 17.94 %.

2) Simulated signal set

The simulated signal set generated by Netcarbench 3.4 is for powertrain subsystem of ACPS, which is composed with 14 ECUs and 100 signals. When security is not considered, the number of the obtained messages is 61 and the bandwidth utilization is 39.36 %.

B. Exploration About the Two Candidate Packing Strategies

We explained in Section IV that there are two candidate packing strategies for SPP (Strategy 2 allows signals with different levels of security requirement to be packed together, while Strategy 1 does not allow that), thus we compared them based on the above two signal sets and the obtained results are shown in Tables III and IV, respectively.

We can find from Tables III and IV that both the obtained number of messages and the bandwidth utilization are smaller for Strategy 2 as compared to Strategy 1. The reason is that compared with the bandwidth overhead brought by increasing the length of MAC to guarantee the security of message, the bandwidth overhead brought by dividing signals with same period into different messages is much bigger. As we analyzed in Section III-A, the bandwidth overhead in CAN message varies from 41.35 % to 97.8 %. Therefore, Strategy 2 is better and employed in SASP from now on.

C. Efficiency of SASP

To show its efficiency, SASP is used to pack the signal sets when the level of security requirement is set as L_1-L_4 for signals, respectively, and the result is shown in Table V and Table VI. We can see from these two tables that along with the increasing of the security requirement, the obtained number of messages and the bandwidth overhead also increase. But as SASP is based on the optimal MILP formulation, even when the level of security requirement reaches L_4, the bandwidth overhead is limited to 5.17 % and 8.22 % for the two signal sets, respectively.

D. Comparison Between SASP and the SPP Algorithm Used in [21]

We did experiments to verify the effectiveness of SASP by comparing it with the SPP algorithm employed in [21]. The SPP algorithm used in [21] is also based on MILP formulation, and we modified its objective function to realize the comparison. As it assumes that the same security requirement is put for all signals, the packing result is the same with that of SASP under the same assumption. Please refer to Tables V and VI for detailed packing result. Tables VII and VIII give the detailed packing result of SASP for the two used signal sets. The runtime of the experiments on SAE signal set and the simulated signal set are about 0.5 s and 4 min, respectively.

We can come to two conclusions from packing result of SASP shown in Tables VII and VIII: 1) horizontal trend, the bandwidth utilization decreases as the percentage of signals with relatively low level of security requirement increases; 2) vertical trend, the bandwidth utilization increases as the widening of the gap between the two levels of security requirement.

From the obtained packing results described in Table V through Table VIII, we can get the conclusion that SASP is more efficient in bandwidth utilization as compared to the packing algorithm used in [21], and Figs. 2 and 3 show the obtained optimization extent in reducing the bandwidth overhead of SASP for the two used signal sets. According to the comparison result, when different combinations of security requirements are explored, the optimization extent of SASP in bandwidth overhead's reduction varies from 10.99 % to 17.8 % and 12.13 % to 49.4 % for the used two signal sets, respectively. With the increasing of the percentage of signals with relatively low level of security requirement, the optimization extent increases; and with the widening of the gap between the two levels of security requirement, the optimization extent also increases.

Taking all the experimental results into account, and considering the facts about the integration of functions with several criticalities into the same ECU and the percentage of functions with high security requirement are relatively low, the usefulness of SASP is obvious for ACPS.

VI. CONCLUSION

We use MAC-based mechanism to defend CAN from masquerade attack, but this mechanism brings bandwidth overhead

TABLE III
COMPARISON RESULT FOR THE TWO PACKING STRATEGIES BASED ON THE SAE SIGNAL SET

The ratio for signals with two levels of security req. (L_2: L_3)		1/3	1	3
Stragety 1	Num of messages	28	27	28
	Bandwidth utilization (%)	28.03	27.6	27.6
Stragety 2	Num of messages	18	18	18
	Bandwidth utilization (%)	21.62	21.6	21.6

TABLE IV
COMPARISON RESULT FOR THE TWO PACKING STRATEGIES BASED ON THE SIMULATED SIGNAL SET

The ratio for signals with two levels of security req. (L_2: L_3)		1/3	1	3
Stragety 1	Num of messages	73	72	72
	Bandwidth utilization (%)	49.48	48.76	48.18
Stragety 2	Num of messages	61	61	61
	Bandwidth utilization (%)	45.04	44.8	44.16

in the meantime. Thus, we formulate a MILP-based optimization problem to realize the tradeoff among the security, real-time and bandwidth utilization for the SPP of CAN. First, we give a new mixed-security signal model to formally describe the properties and requirement in security and real-time at the same time. And then, a MILP-based security-aware signal packing algorithm SASP is proposed, which can realize the optimization of the bandwidth utilization while meeting the requirements in both security and real-time. SASP is also compatiable with the existing CAN specification, which makes it feasible for implementation in real applications. Two sets of experiments based on signal sets from both the industry and simulation tool are implemented to compare the SASP with the state-of-the-art algorithm, and the effectiveness and efficiency of the SASP is showed.

TABLE V
PACKING RESULT OF SAE SIGNAL SET WITH FOUR LEVELS OF SECURITY REQUIREMENT SEPARATELY

Level of security req.	L_1	L_2	L_3	L_4
Num of messages	17	18	18	20
Bandwidth utilization (%)	19.19	20.67	21.93	23.67
Bandwidth overhead (%)	1.25	2.73	3.99	5.17

TABLE VI
PACKING RESULT OF SIMULATED SIGNAL SET WITH FOUR LEVELS OF SECURITY REQUIREMENT SEPARATELY

Level of security req.	L_1	L_2	L_3	L_4
Num of messages	61	61	61	61
Bandwidth utilization (%)	41.42	43.48	45.52	47.68
Bandwidth overhead (%)	2.06	4.12	6.16	8.22

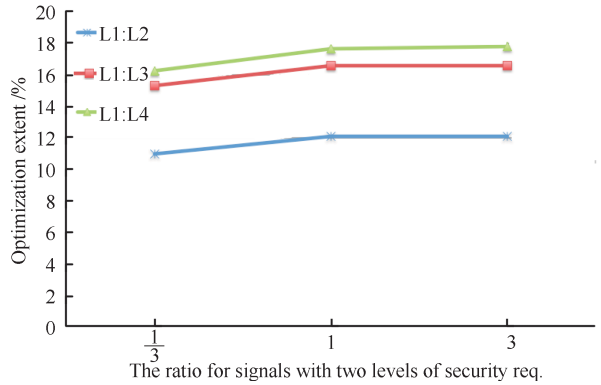


Fig. 2. The optimization extent of SASP compared with the SPP algorithm used in [21] based on SAE signal set.

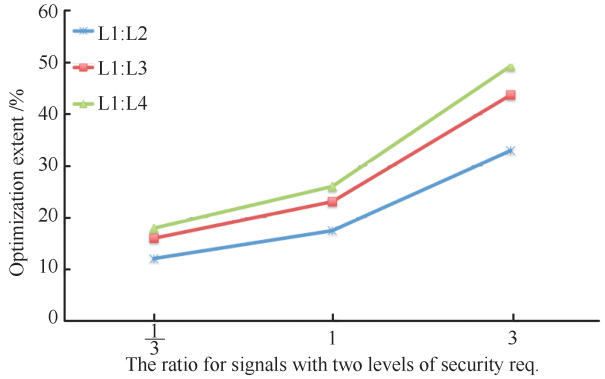


Fig. 3. The optimization extent of SASP compared with the SPP algorithm used in [21] based on the simulated signal set.

TABLE VII
PACKING RESULT OF SASP FOR DIFFERENT COMBINATIONS OF SECURITY REQUIREMENT BASED ON SAE SIGNAL SET

The ratio for signals with two levels of security req.	1/3	1	3
Different combinations of two levels of security req. $(L_1: L_2)(\%)$	20.37	20.34	20.34
Different combinations of two levels of security req. $(L_1: L_3)(\%)$	21.32	21.27	21.27
Different combinations of two levels of security req. $(L_1: L_4)(\%)$	22.27	22.2	22.19

TABLE VIII
PACKING RESULT OF SASP FOR DIFFERENT COMBINATIONS OF SECURITY REQUIREMENT BASED ON SIMULATED SIGNAL SET

The ratio for signals with two levels of security req.	1/3	1	3
Different combinations of two levels of security req.$(L_1: L_2)(\%)$	42.96	42.76	42.12
Different combinations of two levels of security req. $(L_1: L_3)(\%)$	44.54	44.1	42.82
Different combinations of two levels of security req. $(L_1: L_4)(\%)$	46.1	45.44	43.52

REFERENCES

[1] Furst S. Challenges in the design of automotive software. In: Proceedings of the 2010 Design, Automation and Test in Europe Conference and Exhibition (DATE). Dresden: IEEE, 2010. 256−258

[2] Mixed Criticality Systems. EC workshop on mixed crticality systems [Online], available: http://cordis.eurpa.eu, February 3, 2012.

[3] Li R F, Xie Y, and etc. Survery of cyber-physical systems. *Journal of Research and Development*, 2012, **49**(6): 1149−1161 (in Chinese)

[4] Sagstetter F, Lukasiewycz M, Steinhorst S, Wolf M, Bouard A, Harris W R, Jha S, Peyrin T, Poschmann A, Chakraborty S. Security challenges in automotive hardware/software architecture design. In: Proceedings of the 2013 Design, Automation, and Test in Europe Conference and Exhibition (DATE). Grenoble, France: IEEE, 2013. 458−463

[5] Studnia I, Nicomette V, Alata E, Deswarte Y, Kaaniche M, Laarouchi Y. Security of embedded automotive networks: state of the art and a research proposal. In: Proceedings of the 2nd Work-

shop on Open Resilient Human-Aware Cyber-Physical Systems [Online], available: http://hal.archives-ouvertes.fr/doc/00/84/82/34/PDF/4_-_cars_istudnia.pdf, July 25, 2013.

[6] Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S. Comprehensive experimental analyses of automotive attack surfaces. In: Proceedings of the 20th USENIX Conference on Security [Online], available: https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf, August 8, 2011.

[7] Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S. Experimental security analysis of a modern automobile. In: Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP). Oakland, CA: IEEE, 2010. 447−462

[8] Tuohy S, Glavin M, Hughes C, Jones E, Trivedi M, Kilmartin L. Intra-vehicle networks: a review. *IEEE Transactions on Intelligent Transportation Systems*, 2015, **16**(2): 534−545

[9] Hoppe T, Kiltz S, Dittmann J. Security threats to automotive CAN networks-practical examples and selected short-term countermeasures. *Reliability Engineering and System Safety*, 2011, **96**(1): 11−25

[10] Nilsson D K, Larson U E, Jonsson E. Efficient in-vehicle delayed data authentication based on compound message authentication codes. In: Proceedings of the 68th IEEE Vehicular Technology Conference. Calgary, BC: IEEE, 2008. 1−5

[11] Groza B, Murvay S, van Herrewege A, Verbauwhede I. LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks. In: Proceedings of the 11th International Conference on Cryptology and Network Security (CANS). Darmstadt: Springer, 2012. 185−200

[12] Van Herrewege A, Singelee D, Verbauwhede I. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. In: Proceedings of the 2011 ECRYPT Workshop on Lightweight Cryptography [Online], available: http://www.researchgate.net/publication/235323481_CANAuth__A_Simple_Backward_Compatible_Broadcast_Authentication_Protocol_for_CAN_bus, January 19, 2015.

[13] Han K, Weimerskirch A, Shin K G. Automotive cybersecurity for in-vehicle communication. *IQT Quarterly*, 2014, **6**(1): 22−25

[14] Sandstrom K, Norstom C, Ahlmark M. Frame packing in real-time communication. In: Proceedings of the 7th International Conference on Real-Time Computing Systems and Applications (RTCSA). Cheju Island: IEEE, 2000. 399−403

[15] Polzlbauer F, Bate I, Brenner E. On extensible networks for embedded systems. In: Proceedings of the 20th IEEE International Conference and Workshops on the Engineering of Computer Based Systems (ECBS). Scottsdale, AZ: IEEE, 2013. 69−77

[16] Polzlbauer F, Bate I, Brenner E. Optimized frame packing for embedded systems. *IEEE Embedded Systems Letters*, 2012, **4**(3): 65−68

[17] Saket R, Navet N. Frame packing algorithms for automotive applications. *Journal of Embedded Computing*, 2006, **2**: 93−102

[18] Pop P, Eles P, Peng Z B. Schedulability-driven frame packing for multi-cluster distributed embedded systems. *ACM Transactions on Embedded Computing Systems*, 2005, **4**(1): 112−140

[19] Zheng W, Zhu Q, Di Natale M, Vincentelli A S. Definition of task allocation and priority assignment in hard real-time distributed systems. In: Proceedings of 28th IEEE International Real-Time Systems Symposium. Tucson, AZ: IEEE, 2007. 161−170

[20] Zhu Q, Yang Y, Scholte E, Di Natale M, Sangiovanni-Vincentelli A. Optimizing extensibility in hard real-time distributed systems. In: Proceedings of the 15th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS). San Francisco, CA: IEEE, 2009. 275−284

[21] Lin C W, Zhu Q, Phung C, Sangiovanni-Vincentelli A. Security-aware mapping for CAN-based real-time distributed automotive systems. In: Proceedings of the 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). San Jose, CA: IEEE, 2013. 115−121

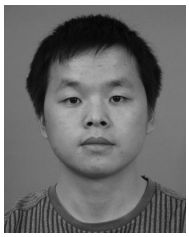
[22] Lin C W, Sangiovanni-Vincentelli A. Cyber-security for the controller area network (CAN) communication protocol. In: Proceedings of the 2012 International Conference on Cyber Security. Washington, DC: IEEE, 2012. 1−7

[23] Davis R I, Burns A, Bril R J, Lukkien J J. Controller area network (CAN) schedulability analysis: refuted, revisited and revised. *Real-Time Systems*, 2007, **35**(3): 239−272

[24] ISO 26262 Road vehicles (2011)-Functional safety [Online], available: http://www.iso.org, August 1, 2014.

[25] Tindell K W, Burns A. Guaranteed message latencies for distributed safety-critical hard real time control networks. In: Proceedings of the 1994 IEEE International Real-Time Systems Symposium (RTSS) [Online], available: http://www.cs.york.ac.uk/ftpdir/reports/YCS-94-229.pdf, August 1, 2014.

[26] NetcarBench 3. 4 [Online], available: http://www.netcarbench.org/, August 1, 2014.



Yong Xie received the Ph. D. degree from Hunan University, China, in 2013. He is currently an assistant professor of Xiamen University of Technology, China. His research interests include automotive embedded systems and cyber-physical systems. Corresponding author of this paper.

Liangjiao Liu Ph. D. candidate at Hunan University. His main research interest is mixed-criticality embedded systems.

Renfa Li received the Ph. D. degree from Tianjin University, China. He is currently a professor of Hunan University. His research interests include embedded systems, cyber-physical systems, and wireless sensor networks.

Jianqiang Hu received the Ph. D. degree from National University of Defensive Technology, China. He is currently an associate professor of Xiamen university of Technology. His research interests include medical embedded system and cloud computing.

Yong Han received the Ph. D. degree from Hunan University, China in 2011. He is currently an associate professor of Xiamen university of Technology. His research interests include automotive crash safety and injury biomechanics.

Xin Peng received the Ph. D. degree from Hunan University, China, in 2011. He is currently an associate professor of Hunan Institute of Science and Technology. His main research interest is automotive communication technologies.