International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1376

(01/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

Security-related misbehaviour detection mechanism using big data for connected vehicles

Recommendation ITU-T X.1376

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	**X.1370–X.1389**
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1376

Security-related misbehaviour detection mechanism using big data for connected vehicles

Summary

Recommendation ITU-T X.1376 describes a security-related misbehaviour detection mechanism for connected vehicles to help stakeholders to utilize automotive data to improve vehicle security.

As connectivity of vehicles increases, the number of vulnerabilities is rising due to the development of complex technology. These vulnerabilities bring more threats to connected vehicles. Analysis of a large amount of automotive data is very useful for assessing security of connected vehicles.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1376	2021-01-07	17	11.1002/1000/14448

Keywords

Connected vehicles, misbehaviour detection.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1376

Security-related misbehaviour detection mechanism using big data for connected vehicles

1 Scope

This Recommendation describes a security-related misbehaviour detection mechanism for connected vehicles. The mechanism includes the following steps.

a) Data capture. Specification of the types of data and information that can be captured from different sources, including automotive, infrastructure, original equipment manufacturers (OEMs) and suppliers, for misbehaviour detection. Data capture methods and procedures lie outside the scope of this Recommendation.

b) Detection. Analysis of the data captured to detect misbehaviour.

This Recommendation applies to connected vehicles to detect misbehaviour by designers and security solution providers. Notification utilization methods lie outside the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 misbehaviour: Act of providing false or misleading data, operating in such a fashion as to impede other service recipients or to operate outside of their authorized scope. Misbehaviour may arise from internal, or external components to the vehicular system.

NOTE 1 – Based on [b-ISO/TR 17427-4].

NOTE 2 – Misbehaviour includes suspicious behaviour as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages, either purposeful or unintended.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADAS Advanced Driver Assistance System

ABS Anti-skid Braking System

AEB Autonomous Emergency Braking

API	Application Programming Interface
CAN	Controller Area Network
GNSS	Global Navigation Satellite System
ITS	Intelligent Transportation System
IP	Internet Protocol
LiDAR	Light Detection and Ranging
MCU	Microcontroller Unit
OEM	Original Equipment Manufacturer
TCU	Telematics Control Unit
URL	Uniform Resource Locator

5 Conventions

None.

6 Model of misbehaviour detection mechanism

Figure 1 provides the model of misbehaviour detection mechanism for connected vehicles. The mechanism includes two steps, data capture and detection, which are implemented by two systems.

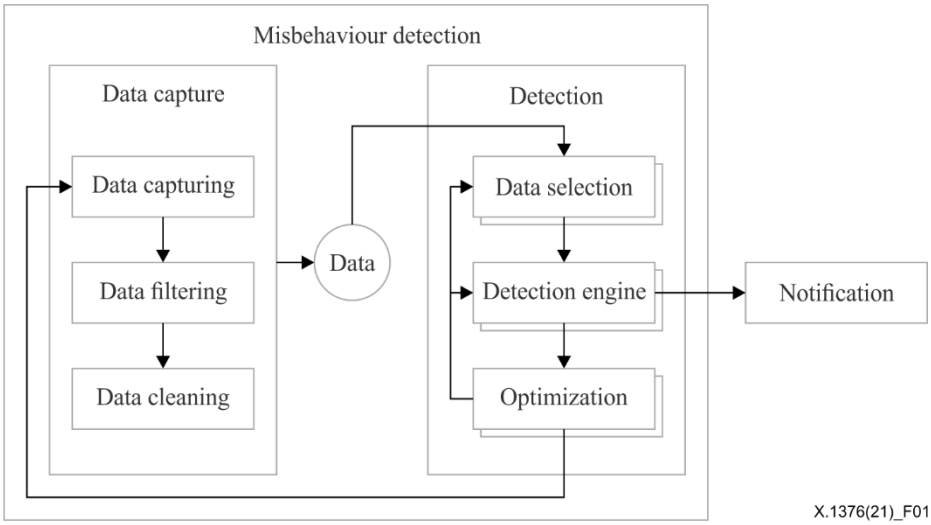

Figure 1 – Model of misbehaviour detection mechanism

Since data capture methods and procedures lie outside the scope of this Recommendation, the data capture system (e.g., data filtering and data cleaning) in Figure 1 is just an informative example of a practical implementation of misbehaviour detection.

Data from the capture system are sent to the detection system, and the data capture processed according to the types described in clause 7.

The data capture system includes the following modules:

a) data collection: collection of data for detection from different sources, e.g., service provider, body system and sensors;

b) data filtering: filter captured data based on data classification;

c) data cleaning: perform deduplication and noise-reduction operations for captured data.

The detection system includes the following modules:

a) data selection: select data sets based on different misbehaviour detection methods, then send them to the detection engine;

b) detection engine: detect misbehaviour based on detection methods, then send decision results to optimization and notification, as appropriate;

c) optimization: use the detection results from the detection engine to improve data selection, detection engine and data capturing.

Notification is a module that sends the outputs from the detection engine to stakeholders. It does not lie within the scope of this Recommendation.

7 Data capture

Data capture usually includes data capturing, data cleaning and data filtering. Since data capture methods and procedures lie outside the scope of this Recommendation, only data types used in the detection procedure are specified. Any personal sensitive data should be protected with proper technologies such as anonymization, which lies outside the scope of this Recommendation.

Based on data and information captured from different sources, this clause specifies the types used in the misbehaviour detection mechanism, namely status data, control data and intelligence data, as shown in Table 1.

Table 1 – Data types

Type	Subtype	Data sources	Data examples
Status data[a]	Application or service data	Content provider or service provider	Infotainment data
		Map service data	Navigation, positioning
		Mobile application data	Application-related data
	Vehicle status	Safety system	Anti-skid braking system (ABS), airbag, autonomous emergency braking (AEB), advanced driver assistance systems (ADASs)
		Body system	Door, window, wiper
		Chassis system	Torque, corner
		Power system	Speed, rotational speed, throttle valve, stalls
	Environmental sensors	Radar	Millimetre wave radar
		Light detection and ranging (LiDAR)	Point cloud
		Ultrasonic sensors	Distance
		Camera	Surrounding image
		Intelligent transportation system (ITS) sensors	Roadside facilities sign
Control data[b]	Local control	In-vehicle controller	Open door, close door
	Remote control	Automation, telematics	Remote diagnosis

Table 1 – Data types

Type	Subtype	Data sources	Data examples
Intelligence data[c]	Internal intelligence data	Security research, testing results	Vulnerabilities, bugs, internal cybersecurity events
	External sharing intelligence data	Customer, supplier, community, conference or literature, web	Internet protocol (IP) address, hash values, uniform resource locator (URL), domain name, common vulnerabilities and exposures (CVE), etc.

[a] Data and information related to the status of vehicles, applications, services, sensors and other facilities in an ITS.

[b] Data and information used to control vehicles, applications, services, sensors and other facilities in an ITS.

[c] Data and information related to cybersecurity obtained from outside an ITS. It is assumed that the sources of the data have the right level of integrity.

8 Detection

The detection module mainly consists of data selection, detection engine and optimization. As shown in Figure 2, based on data and information from different sources, the detection engine uses big data analysis to identify misbehaviour. Optimization uses misbehaviours to optimize data selection and the detection engine makes misbehaviour detection more accurate and efficient.

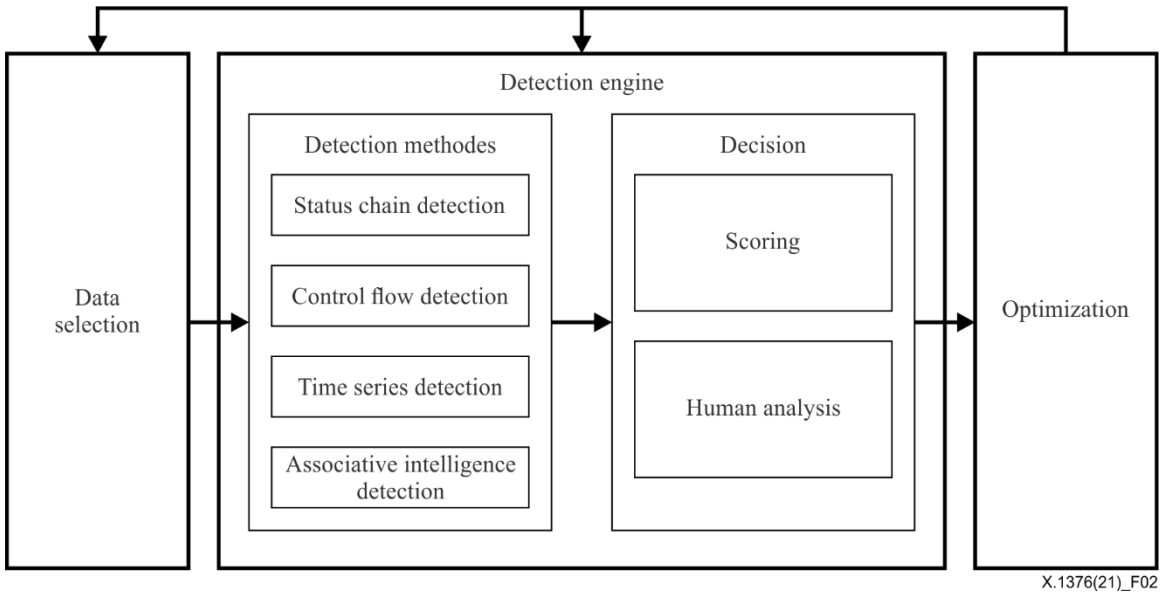

Figure 2 – Procedure of detection

8.1 Data selection

Based on the various data requirements of detection methods, the data selection module classifies data into different data sets according to the requirements of detection engines, as shown in Figure 3. The input into the data selection module is data from the capture system.

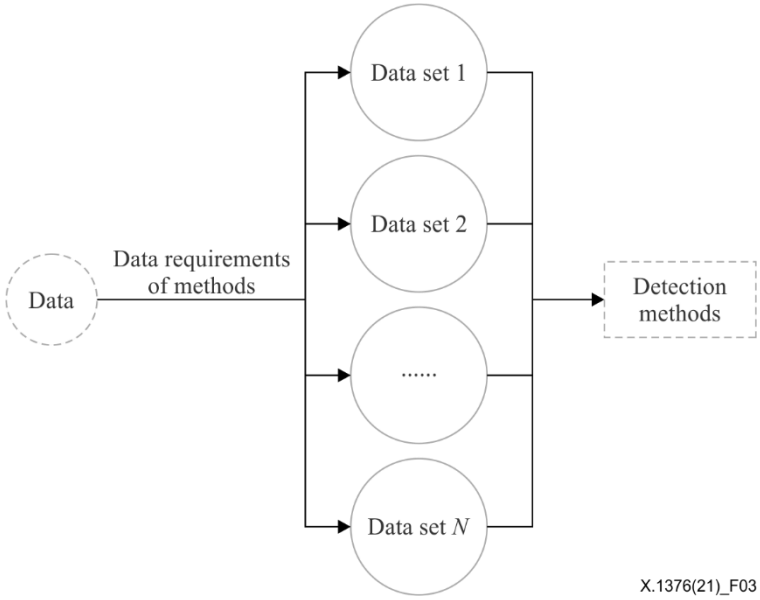

Figure 3 – Procedure of data selection

8.2 Detection engine

The detection engine consists of two submodules: detection methods; and decision. When the data sets come into the detection methods submodule, methods will transform them into behaviour traits. Then the decision submodule makes a decision based on the behaviour traits. Decision results have three different types: blocked; suspicious; and allowed. A blocked result means it is anomalous; a suspicious result means that it cannot be determined whether the data are denied or secure; and an allowed result means the data are secure.

8.2.1 Detection methods

The detection methods submodule is a set of different detection methods. Based on the data types classified in clause 7, four methods have been designed to detect misbehaviour using these data.

8.2.1.1 Status chain detection

The status chain contains a series of correlated status data. In the status chain, change in one datum causes other data to change at the same time.

Some characteristics of a status chain follow:

a) node: a service or an application in an ITS that is relevant to an action;

b) flow: the direction and path of changing data made by an action.

Status data are generated in an ITS and a context can be created with these data. Data value also follows a certain trend and fluctuates within a certain range.

In essence, the status chain can be divided into two models: line and branch. The two models are as follows:

1) line: each node has only one node that receives its signal;

2) branch: one node generates two or more status data at the same time, then sends them to different nodes.

In the line model of a status chain, the nodes only have a one-way connection. See Figure 4.

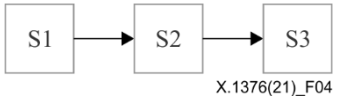

Figure 4 – Line model of status chain
S: status

In the branch model of a status chain, the nodes can be forked into two or more relevant line models. See Figure 5.

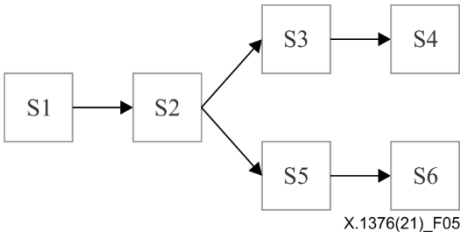

Figure 5 – Branch model of status chain

Thus, the traits of each node include:

i) the context in the status chain;

ii) the value and trend of each node.

The traits from the nodes in the status chain are obtained, and then sent to the scoring function.

8.2.1.2 Control flow detection

The control flow contains a series of correlated control data. In the control flow, one control command can be made up of multiple sub-control-commands and will affect multiple systems.

Some characteristics of control flow to describe control command execution follow:

a) node: a service or an application in the ITS that is relevant to an action;

b) flow: the direction and path of changing data made by an action.

When a control action proceeds, control-related data will pass through control-related nodes and form a control flow.

Every control node works stably and regularly in an ITS. When many nodes work together, the control flow is also stable in behaviour, due to the prescribed period, the determined types and number of messages.

In essence, control flow can be divided into two models: line and branch. The two models are as follows:

1) line: each node has only one node that receives its signal;

2) branch: one node generates two or more control data at the same time, then sends them to different nodes.

In the line model control flow, the nodes only have one-way connection. See Figure 6.

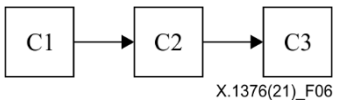

Figure 6 – Line model of control flow
C: control

In the branch model control flow, the nodes can be forked into two or more relevant line models. See Figure 7.

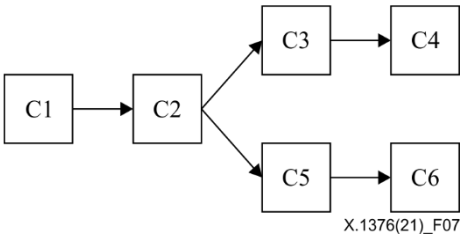

Figure 7 – Branch model of control flow

8.2.1.3 Time series detection

A time series is used to describe data that change according to type. As long as the data are in accordance with the types, then time series detection can be used.

The changing trend of time series data has four types:

a) tendency: the data change with time or independent variables, showing a relatively slow and long-term trend of the same nature of continuous rise, fall or staying the same, but the change range may not be equal;

b) periodicity: a factor gradually shows repeated characteristics over time, including peaks and troughs;

c) randomness: the data are randomly changing, but the overall situation is statistical;

d) superposition: the actual change is a superposition or combination of several changes.

Some characteristics of time series behaviours follow:

1) node: a service or an application in the ITS that is relevant to time series data;

2) flow: indicates time chronologically.

Many data belong to time series data, e.g., controller area network (CAN) messages. The data model can be established with one or more types of data to find the misbehaviour. See Figure 8.

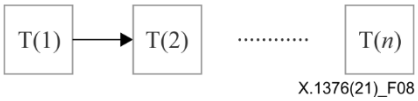

Figure 8 – Line model of time series
T: time

8.2.1.4 Associative intelligence detection

For the associative intelligence detection method, misbehaviour can be detected directly or indirectly. Associative intelligence data can therefore be divided into two categories: direct and indirect.

Direct associative intelligence: misbehaviour can be detected directly based on this intelligence, e.g., external vulnerabilities report, internal cybersecurity research and common vulnerabilities disclosure.

Indirect associative intelligence: misbehaviour cannot be detected directly based on this intelligence, since such intelligence is used to describe normal events, e.g., bug fixing, new feature release, software update and chip replacement. Combining indirect associative intelligence with other data captured, misbehaviour can be detected.

8.2.2 Decision

This clause introduces the decision submodule procedure shown in Figure 9.

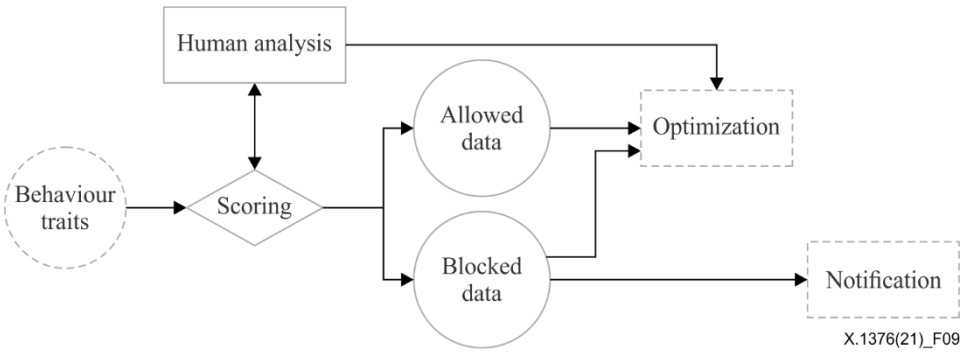

Figure 9 – Procedure in decision submodule

The decision submodule is used to determine the results from detection methods. It includes two functions: scoring and human analysis. The scoring function determines the data type by behaviour traits, then scores it. If misbehaviour such as a hijacking or tampering attack happens, it deviates from the stability baseline. If the score cannot meet the allowed or blocked threshold, it will be classed as suspicious. Human analysts will then intervene and help to make a decision until the score meets the allowed or blocked threshold.

8.3 Optimization

Optimization is a feedback module, which receives data from the detection engine and uses them to optimize it. See Figure 10.

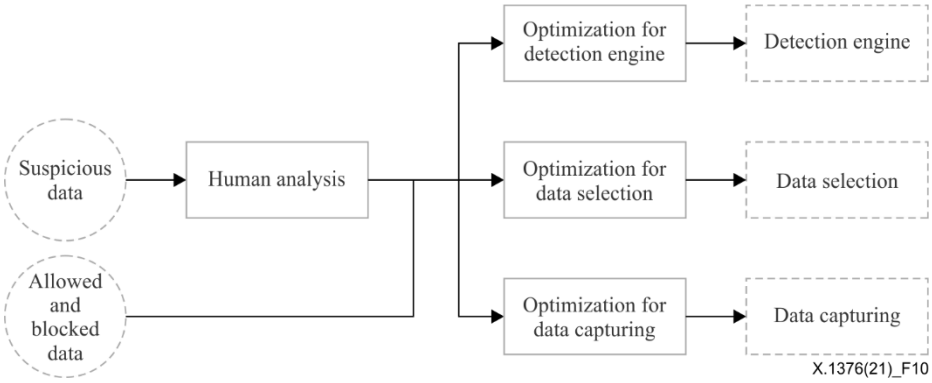

Figure 10 – Procedure in optimization

8.3.1 Optimization for detection engine

The trait is the key value in every transmitted datum in the flow. At the beginning of misbehaviour detection, stability baselines are generated by normal traits from the normal environment. The scoring function is initialized.

The detection engine is optimized by its outputs. Detection methods are added, modified or deleted in order to improve detection efficiency; the scoring function is also optimized by the addition of new knowledge derived from human analysis.

8.3.2 Optimization for data selection

The data sets are added, modified or deleted in order to improve detection accuracy.

8.3.3 Optimization for data capturing

The data captured are added, modified or deleted in order to improve detection accuracy.

Appendix I

Use cases of different detection methods

(This appendix does not form an integral part of this Recommendation.)

This appendix provides use cases of how to detect misbehaviour according to different detection methods in clause 8.2.1.

I.1 Status chain case

This is a status chain detection case for clause 8.2.1.1.

A vehicle has a communication module to get access to the Internet called a telematics control unit (TCU). A TCU does not run all the time, so it switches into low power mode after the engine of vehicle is stopped to save power. Before the low power mode, it sends the status of vehicle to the vehicle gateway (backend service), which synchronizes this status to the TCU status cache. The command service then gets this status from the TCU status cache. When a user sends a command to their vehicle, the command service reacts according to the TCU status. If the TCU is in the low power mode, the command service sends a request to the wakeup service, which then wakes up the TCU. Figure I.1 shows normal behaviour. Table I.1 shows the status data involved in this normal behaviour.

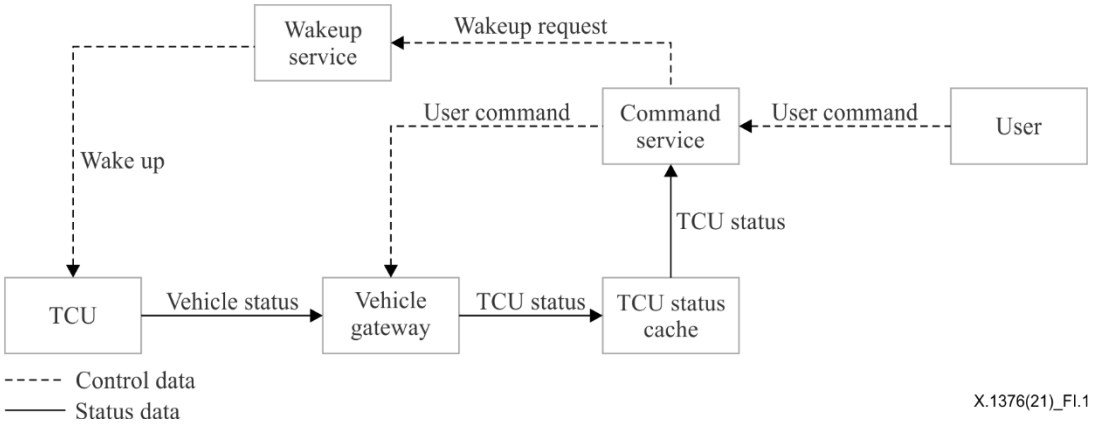

Figure I.1 – Normal behaviour of status chain

When attackers want to figure out this procedure, they will try to modify the TCU status to see the different behaviours that the command service exhibits. There will then be a difference between the TCU status cache and the vehicle gateway.

In this case, status chain detection can detect misbehaviour by comparing the vehicle status in the vehicle gateway and the TCU status in the TCU status cache. If their statuses are different, this is a misbehaviour. The TCU cannot be in low power mode when the vehicle is running.

Table I.1 – Vehicle driving status data

Node	Data
Vehicle gateway	Vehicle status
TCU status cache	TCU status
Command service	TCU status

I.2 Control flow case

This is a control flow detection case for clause 8.2.1.2.

When a user wants to control the vehicle remotely, it is necessary to use the application installed on the user's smartphone to trigger the function. The application will generate an operation log. Then the application will send a request to the back-end application programming interface (API) service, which will record this request in the access log. The API service will then pre-treat the request and forward it to the vehicle endpoint, e.g., the TCU. The TCU will invoke a microcontroller unit (MCU) with the transceiver and send a command to the relevant executor. Finally, the actuator will execute the control command from the user side. See Figure I.3. Table I.2 shows the control data involved in this normal behaviour.

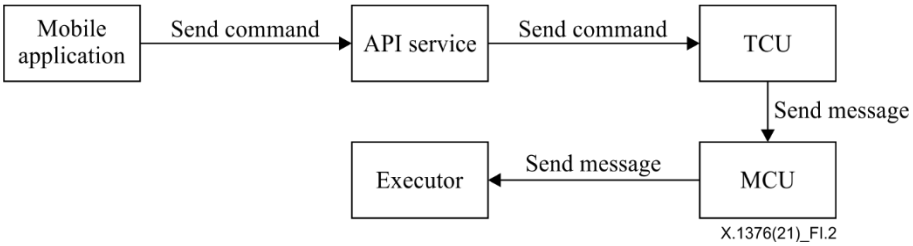

Figure I.2 – Normal behaviour of control flow

In this case, the TCU sends messages to the MCU only when the API service asks. If the MCU is invoked from an abnormal path, there will be no operation log in the mobile application and API service. Then misbehaviour is detected.

Table I.2 – Telematics control data

Node	Data
Mobile application	Operation log
API service	Access log
TCU	Received data
MCU	Invoking log
Executor	Executor log

I.3 Time series case

This is a time series detection case for clause 8.2.1.3.

In this case, the TCU sends the position of the vehicle to the backend service periodically. See Figure I.3.

Latitude (°)	Interval (s)
39.9544	10.4015592431
39.9566	10.2439587253
39.9594	10.5735141799
39.9502	10.3234362303
39.9528	10.0973092011
39.9538	10.5066656864
39.9558	10.4945798327
39.9556	10.1209659368
39.9506	10.2163646279
39.9551	10.1042228459

Figure I.3 – Normal time series of position

If a global navigation satellite system (GNSS) sensor is in a spoofing situation, the position information and interval will have an obvious difference to previous data. See Figure I.4.

Latitude (°)	Interval (s)
39.9503	10.4741553595
39.9595	10.2682504585
39.9597	10.2750387130
39.9568	10.4752930715
39.9520	10.6371744699
45.1525	5.4110037357
39.9597	5.5768263688
39.9508	10.4367481108
39.9550	10.0731090275
39.9529	10.5550728359
39.9518	10.5853553005
39.9554	10.1983262711

Figure I.4 – Misbehaviour time series of position

Table I.3 shows the common time series data in the vehicle.

Table I.3 – Automated sensor time series data

Node	Data
Backend Service	Latitude, interval

I.4 Associative intelligence detection case

There are two associative intelligence detection cases for clause 8.2.1.4, so two use cases are provided, one for each.

I.4.1 Direct associative intelligence detection case

Detecting misbehaviour based on direct associative intelligence is the easier way in a connected vehicle. All forms of direct associative intelligence point to misbehaviour directly, e.g., IP address, domain name, URL, internal cybersecurity research and external vulnerabilities report. Any of these data include an absolute trait to detect misbehaviour.

Table I.4 shows the common direct associative intelligences in the ITS.

Table I.4 – Direct associative intelligence detection data

Node	Data
In-vehicle infotainment system	IP address URL Domain name
Intelligence database	External vulnerabilities report Internal cybersecurity research

I.4.2 Indirect associative intelligence detection case

Indirect associative intelligence cannot be used to detect misbehaviour independently, but it can be combined with other intelligence sources. In some circumstances, a single vulnerability cannot be exploited, but an attacker can utilize several vulnerabilities to build an exploitation chain to achieve exploitation. For example, not every vendor fixes vulnerabilities so that they cannot be exploited. When the detection engine receives a new technical report about chaining, [b-CVE-2017-11906] and [b-CVE-2017-11907] can reach arbitrary code execution; the version of the browser in the in-vehicle infotainment system is captured for use together with intelligent data to detect misbehaviour.

Table I.5 shows the common indirect associative intelligences in the ITS.

Table I.5 – Indirect associative intelligence detection data

Node	Data
Intelligence database	In-vehicle infotainment system External technical report

Bibliography

[b-ISO/TR 17427-4] ISO/TR 17427-4:2015, *Intelligent transport systems – Cooperative ITS – Part 4: Minimum system requirements and behaviour for core systems*.

[b-CVE-2017-11906] Common Vulnerabilities and Exposures, CVE-2017-11906 (2017). *Internet Explorer information disclosure vulnerability*. Bedford, MA: Mitre Corporation. Available [viewed 2021-02-21] at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906

[b-CVE-2017-11907] Common Vulnerabilities and Exposures, CVE-2017-11907 (2017). *Scripting engine memory corruption vulnerability*. Bedford, MA: Mitre Corporation. Available [viewed 2021-02-21] at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021