ETSI TR 102 893 V1.2.1 (2017-03)

TECHNICAL REPORT

Intelligent Transport Systems (ITS);
Security;
Threat, Vulnerability and Risk Analysis (TVRA)

Reference

RTR/ITS-0050018

Keywords

authentication, authorization, confidentiality, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of 5,9 GHz radio communications in an Intelligent Transport System (ITS). The analysis considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) [i.3] operating in a fully deployed ITS.

The present document was prepared using the TVRA method described in ETSI TS 102 165-1 [i.1].

NOTE: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the ETSI ITS Work Programme.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.2] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

[i.3] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

[i.4] IEEE 802.11TM: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.5] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.6] IETF RFC 4120: "The Kerberos Network Authentication Service (V5)".

NOTE: Available at http://tools.ietf.org/html/rfc4120.

[i.7] ETSI TS 102 636-4-1: "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.8] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.9] ETSI TR 102 863: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization".

[i.10] ETSI EN 302 636-4-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.11] Risk analysis study of ITS communication architecture, R Moalla, H Labiod, B Lonc, N Simoni, IEEE Network of the Future conference, 2012.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

beaconing: network layer service which retransmits requested information

end user: functional agent directly representing the human user of the ITS or the ITS service provider

geo-addressing: network layer service that enables the addressing a specific geographic region

ITS application: entity that defines and implements an ITS use case or a set of ITS use cases

ITS use case: specific scenario in which ITS messages are exchanged

ITS user: any ITS application or functional agent sending, receiving or accessing ITS-related information

local dynamic map: dynamically maintained information on driving and environmental conditions in the vicinity of the ITS-S

restricted local ITS station data: data to be shared only with authorized parties

unrestricted local ITS station data: data that may be shared without requiring authorization from the recipient

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Attribute Authority
AC	Attribute Certificate
BSA	Basic Set of Applications
CA	Co-operative Awareness
CAM	Cooperative Awareness Message
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
CN	Co-operative Navigation
CS	Communities Services
CSM	Co-operative Speed Management
DENM	Decentralized Environmental Notification Message
DNM	Decentralized environmental Notification Message
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
FA	Functional Asset
FM	Frequency Modulation
GAC	GeoAnycast
GBC	GeoBroadcast
GNSS	Global Navigation Satellite System
GUC	GeoUnicast
HMAC	Hashed Message Authentication Code

HMI	Human-Machine Interface
I2V	Infrastructure to Vehicle
IAAA	Identification, Authentication, Authorization, Accountability
INS	Inertial Navigation System
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-S	ITS Station
LBS	Location Based Services
LCM	Life Cycle Management
LDM	Local Dynamic Map
OS	Operating System
PKI	Public Keying Infrastructure
PMI	Privilege Management Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
SAML	Security Assertion Markup Language
SFR	Security Functional Requirement
SHB	Single-Hop Broadcast
SoA	Source of Authority
SSP	Service Specific Permissions
ToE	Target of Evaluation
TSB	Topologically-Scoped Broadcast
TTP	Trusted Third Party
TVRA	Threat, Vulnerability and Risk Analysis
UTC	Universal Coordinated Time
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VIN	Vehicle Identification Number

4 The TVRA Method

Without an understanding of the threats posed to a system it is impossible to select or devise appropriate measures to counter these threats. The ETSI Threat, Vulnerability and Risk Analysis (TVRA) [i.1] is used to identify risks to a system by isolating the vulnerabilities of the system, assessing the likelihood of a malicious attack on that vulnerability and determining the impact that such an attack will have on the system.

The TVRA method process consists of the following steps:

1) Identification of the Target of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.

10) Specification of detailed requirements for the security services and capabilities from step 9.

The present document summarizes the results from each of these steps in the analysis of the ETSI Intelligent Transport System (ITS) standards.

5 The ETSI Intelligent Transport System

5.1 ITS architecture

5.1.1 General

The ITS security architecture is defined in ETSI TS 102 940 [i.8] and covers both the Communication Architecture and the architecture of the ITS-S itself. ETSI TR 102 638 [i.3] defines the basic set of ITS applications which it divides into groups according to the functionality provided which is further analysed in ETSI TR 102 863 [i.9] and transformed into a detail classification of ITS applications in ETSI TS 102 940 [i.8]. For ease of reading and for further risk analysis the relevant tables from ETSI TS 102 940 [i.8] are copied here.

Table 1: ITS application classes

Applications Class	Application	Use case
Active road safety	Driving assistance - Co-operative Awareness (CA)	Emergency vehicle warning
		Slow vehicle indication
		Across traffic turn collision risk warning
		Merging Traffic Turn Collision Risk Warning
		Co-operative merging assistance
		Intersection collision warning
		Co-operative forward collision warning
		Lane Change Manoeuvre
	Driving assistance - Road Hazard Warning (RHW)	Emergency electronic brake lights
		Wrong way driving warning (infrastructure based)
		Stationary vehicle - accident
		Stationary vehicle - vehicle problem
		Traffic condition warning
		Signal violation warning
		Roadwork warning
		Decentralized floating car data - Hazardous location
		Decentralized floating car data - Precipitations
		Decentralized floating car data - Road adhesion
		Decentralized floating car data - Visibility
		Decentralized floating car data - Wind
		Vulnerable road user Warning
		Pre-crash sensing warning
		Co-operative glare reduction
Cooperative traffic efficiency	Co-operative Speed Management (CSM)	Regulatory/contextual speed limits notification
		Curve Warning
		Traffic light optimal speed advisory
	Co-operative Navigation (CN)	Traffic information and recommended itinerary
		Public transport information
		In-vehicle signage

Applications Class	Application	Use case
Co-operative local services	Location Based Services (LBS)	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet services	Communities Services (CS)	Insurance and financial services
		Fleet management
		Loading zone management
		Theft related services/After theft vehicle recovery
	ITS station Life Cycle Management (LCM)	Vehicle software/data provisioning and update
		Vehicle and RSU data calibration
	Transport related electronic financial transactions (road tolls)	

5.1.2 Summary of ITS applications

In order to define security classes the communication patterns of the different applications also need to be considered. Table 2 summarizes the communication behavior of each application.

Table 2: ITS applications communication behavior

Use case		Addressing	Hops	Frequency	Direction	Session
Emergency vehicle warning		Broadcast	Single	High	V2V/V2I	No
Slow vehicle indication		Broadcast	Single	High	V2V	No
Across traffic turn collision risk warning		Broadcast	Single	High	V2V	No
Merging Traffic Turn Collision Risk Warning		Broadcast	Single	High	V2V/I2V	No
Co-operative merging assistance		Broadcast	Single	High	V2V/I2V	No
Intersection collision warning		Broadcast	Single	High	V2V/I2V	No
Co-operative forward collision warning		Broadcast	Single	High	V2V	No
Lane Change Manoeuvre		Broadcast	Single	High	V2V	No
Emergency electronic brake lights		Broadcast	Multi	Low	V2V	No
Wrong way driving warning (infrastructure based)		Broadcast	Single	Low	I2V	No
Stationary vehicle - accident		Broadcast	Multi	Low	V2V/V2I	No
Stationary vehicle - vehicle problem		Broadcast	Multi	Low	V2V/V2I	No
Traffic condition warning		Broadcast	Multi	Low	V2V/I2V	No
Signal violation warning		Broadcast	Single	High	I2V	No
Roadwork warning		Broadcast	Multi	Low	I2V	No
Decentralized floating car data - Hazardous location		Broadcast	Multi	Low	V2V/I2V	No
Decentralized floating car data - Precipitations		Broadcast	Multi	Low	V2V	No
Decentralized floating car data - Road adhesion		Broadcast	Multi	Low	V2V	No
Decentralized floating car data - Visibility		Broadcast	Multi	Low	V2V	No
Decentralized floating car data - Wind		Broadcast	Multi	Low	V2V	No
Vulnerable road user Warning		Broadcast	Single	Low	V2V/I2V	No
Pre-crash sensing warning	Indication	Broadcast	Single	High	V2V	No
	Data exchange	Unicast	Single	High	V2V	Yes
Co-operative glare reduction		Broadcast	Single	Low	V2V/I2V	No
Regulatory/contextual speed limits notification		Broadcast	Single	Low	I2V	No
Curve Warning		Broadcast	Single	Medium	I2V	No
Traffic light optimal speed advisory		Broadcast	Multi	Medium	I2V	No
Traffic information and recommended itinerary	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Unicast/Multicast	Multi	Medium	I2V	Yes
Public transport information	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Multicast	Multi	Medium	I2V	Yes
In-vehicle signage		Broadcast	Single	Medium	I2V	No
Point of Interest notification	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Multicast	Single	Low	I2V	Yes

Use case		Addressing	Hops	Frequency	Direction	Session
Automatic access control and parking management	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Unicast	Single	Low	I2V/V2I	Yes
ITS local electronic commerce		Unicast	Single	Low	I2V/V2I	Yes
Media downloading		Unicast	Single	Low	I2V/V2I	Yes
Insurance and financial services		Unicast	Single	Low	I2V/V2I	Yes
Fleet management		Unicast	Single	Low	I2V/V2I	Yes
Loading zone management		Unicast/Multicast	Single	Low	I2V/V2I	Yes
Theft related services/After theft vehicle recovery		Unicast	Multi	Low	I2V/V2I	Yes
Vehicle software/data provisioning and update		Unicast	Single	Low	I2V/V2I	Yes
Vehicle and RSU data calibration		Unicast	Single	Low	I2V/V2I	Yes

The information in Table 2 makes it possible to define a number of ITS application categories, thus:

- cooperative awareness;
- static local hazard warnings;
- interactive local hazard warnings;
- area hazard warnings;
- advertised services;
- local high-speed unicast services;
- local multicast services;
- low-speed unicast services; and
- distributed (networked) services.

6 ITS Security Objectives

6.1 Confidentiality

The following security objectives related to the confidentiality of stored and transmitted ITS information are specified:

Co1. Information sent to or from an authorized ITS user should not be revealed to any party not authorized to receive the information.

Co2. Information held within the ITS-S should be protected from unauthorized access.

Co3. Details relating to the identity and service capabilities of an ITS user should not be revealed to any unauthorized 3rd party.

Co4. Management Information sent to or from an ITS-S should be protected from unauthorized access.

Co5. Management Information held within an ITS-S should be protected from unauthorized access.

Co6. It should not be possible for an unauthorized party to deduce the location or identity of an ITS user by analysing communications traffic flows to and from the ITS user's vehicle.

Co7. It should not be possible for an unauthorized party to deduce the route taken by an ITS end-user by analysing communications traffic flows to and from the ITS end-user's vehicle.

6.2 Integrity

The following security objectives related to the integrity of stored and transmitted ITS information are specified:

In1. Information held within an ITS-S should be protected from unauthorized modification and deletion.

In2. Information sent to or from a registered ITS user should be protected against unauthorized or malicious modification or manipulation during transmission.

In3. Management Information held within a ITS-S should be protected from unauthorized modification and deletion.

In4. Management Information sent to or from an ITS-S should be protected against unauthorized or malicious modification or manipulation during transmission.

6.3 Availability

The following security objectives related to the availability of ITS services are specified:

Av1. Access to and the operation of ITS services by authorized users should not be prevented by malicious activity within the ITS-S environment.

6.4 Accountability

The following security objectives related to the accountability of ITS users are specified:

Ac1. It should be possible to audit all changes to security parameters and applications (updates, additions and deletions).

6.5 Authenticity

The following security objectives related to the authenticity of ITS users and transmitted information are specified:

Au1. It should not be possible for an unauthorized user to pose as an ITS-S when communicating with another ITS-S.

Au2. It should not be possible for an ITS-S to receive and process management and configuration information from an unauthorized user.

Au3. Restricted ITS services should be available only to authorized users of the ITS.

7 ITS Functional Security classes

7.1 Confidentiality

The identified functional security classes (SFRs) specified in Table 3 together meet the confidentiality objectives identified in clause 6.1.

Table 3: Identified functional security classes associated with confidentiality

Objective		Functional Security Requirements
ID	**Text**	
Co1	Information sent to or from an authorized ITS user should not be revealed to any party not authorized to receive the information	An ITS system should provide a means of designating certain information as restricted
		Restricted information sent to and from an authorized ITS user should be encrypted
		Before transmitting restricted information to another user, an ITS user should authenticate itself to the recipient
		Before receiving restricted information from another user, an ITS user should be required to authenticate itself to the sender
Co2	Information held within an ITS-S should be protected from unauthorized access	An ITS-S should permit only authorized ITS applications to access its security parameter information
		An ITS-S should permit only authorized ITS users to access its restricted information
Co3	Details relating to the identity and service capabilities of an ITS user should not be revealed to any unauthorized 3rd party	The functional security requirements specified for objective Co2 satisfy the needs of objective Co3

Objective		Functional Security Requirements
ID	**Text**	
Co4	Management Information sent to or from an ITS-S should be protected from unauthorized access	An ITS-S should permit only authorized ITS users to install management information such as service profile data and software updates
		An ITS-S should only accept management information from an authorized source
		An ITS-S should restrict access to transmitted management information to authorized ITS users
Co5	Management Information held within an ITS-S should be protected from unauthorized access	An ITS-S should restrict access to stored management information such as service profile data and software updates, to authorized ITS users
		An ITS-S should provide a means designating an ITS user as authorized to access to stored management information
Co6	It should not be possible for an unauthorized party to deduce the location and identity of an ITS end-user by analysing communications traffic flows to and from the ITS end-user's vehicle	An ITS-S should not include a persistent user identity with location data to an unlimited multicast address
		An ITS-S may include a persistent user identity with location data sent to a unicast or limited multicast address
		An ITS-S should have the means to protect location and identity information during transmission
Co7	It should not be possible for an unauthorized party to deduce the route taken by an ITS end-user by analysing communications traffic flows to and from the ITS end-user's vehicle	An ITS-S should have the means to use multiple identifiers
		Where multiple identifiers are used, an ITS-S should provide a means of ensuring that no mathematical or syntactical link should exist between identifiers

7.2 Integrity

The identified functional security classes (SFRs) specified in Table 4 together meet the integrity objectives identified in clause 6.2.

Table 4: Identified functional security classes associated with integrity

Objective		Functional Security Requirements
ID	**Text**	
In1	Information held within an ITS-S should be protected from unauthorized modification and deletion	An ITS-S should permit only authorized ITS applications to modify or delete its security parameter and LDM information
		An ITS-S should permit only authorized ITS applications and authorized ITS users to modify or delete Service profile information
In2	Information sent to or from an registered ITS user should be protected against unauthorized or malicious modification or manipulation during transmission	An ITS-S should implement one or more methods to enable it, if requested by an ITS user, to detect en route modification or manipulation of received data
		An ITS-S should implement one or more methods for preventing the modification or manipulation of data that it transmits or receives
In3	Management Information held within a ITS-S should be protected from unauthorized modification and destruction	The functional security requirements specified for objective In1 satisfy the needs of objective In3
In4	Management Information sent to or from an ITS-S should be protected against unauthorized or malicious modification or manipulation during transmission	The functional security requirements specified for objective In2 satisfy the needs of objective In4

7.3 Availability

The identified functional security classes (SFRs) specified in Table 5 together meet the availability objectives identified in clause 6.3.

Table 5: Identified functional security classes associated with availability

Objective		Functional Security Requirements
ID	Text	
Av1	Access to and the operation of ITS services by authorized users should not be prevented by malicious activity within the ITS-S environment	An ITS-S should be able to detect easily recognizable Denial of Service attack patterns

7.4 Accountability

The identified functional security classes (SFRs) specified in Table 6 together meet the accountability objectives identified in clause 6.4.

Table 6: Identified functional security classes associated with accountability

Objective		Functional Security Requirements
ID	Text	
Ac1	It should be possible to audit all changes to security parameters and applications (updates, additions and deletions)	An ITS-S should record all requests for changes to security parameter information and ITS applications
		An ITS-S should record the results of all requests for changes to security parameter information and ITS applications

7.5 Authenticity

The identified functional security classes (SFRs) specified in Table 7 together meet the authenticity objectives identified in clause 6.5.

Table 7: Identified functional security classes associated with authenticity

Objective		Functional Security Requirements
ID	Text	
Au1	It should not be possible for an unauthorized ITS user to pose as an ITS-S when communicating with other ITS-Ss	Only an authorized ITS-S should have access to emergency vehicle services
		An ITS-S should have the means to validate the identity of an authorized emergency vehicle
		It should be possible for an ITS-S installed in a private vehicle to be given authority to access emergency vehicle services on a temporary basis
		An ITS-S installed in an emergency vehicle (permanent or temporary) should have the means to positively identity itself as such
		An ITS-S should be permitted to send an ITS message only if suitably authorized
		An ITS-S should reject an incoming ITS message received from an unauthorized source
Au2	It should not be possible for an ITS-S to receive and process management and configuration information from an unauthorized user	The functional security requirements specified for objective In1 satisfy the needs of objective Au2
Au3	Restricted ITS services (Emergency Vehicle Warning) should be available only to authorized ITS users	An ITS-S should permit only currently authorized ITS users to transmit messages identifying the vehicle as an emergency vehicle
		An ITS user's authorization to transmit messages identifying the vehicle as an emergency vehicle may be time limited by expiry or explicit removal

8 ITS Target of Evaluation (ToE)

8.1 General

From the architectural descriptions in clause 5 it is possible to identify two potential Targets of Evaluation (ToE) for security analysis purposes:

- a single ITS-S (Vehicle) as shown in Figure 1;
- a single ITS-S (Roadside) as shown in Figure 2.

A ToE is defined such that all potential attack interfaces are exposed; i.e. each interface has one end-point inside the ToE and one end-point outside of the ToE boundaries. A ToE can only be attacked through its exposed interfaces and the presence of a threat agent is necessary to launch an attack. This means that the assets (most often the functional entities) associated with the exposed interfaces are potential threat agents and that the ToE environment should include all exposed interfaces and all assets associated with the end-points of these interfaces that are outside the ToE.

The scope of this analysis is communication over 5,9 GHz (ITS G5A). This means that only the interfaces at A and B are within scope. In the ITS-S (Vehicle) case (see Figure 1), the interfaces at both A and B are exposed and the ToE environment includes the two interfaces and their end-points in other ITS-S (Vehicle)s and ITS-S (Roadside)s within range at any given point in time. Only the assets associated with the ITS-S (Vehicle) and ITS-S (Roadside) are potential threat agents or can be used as attack proxies.

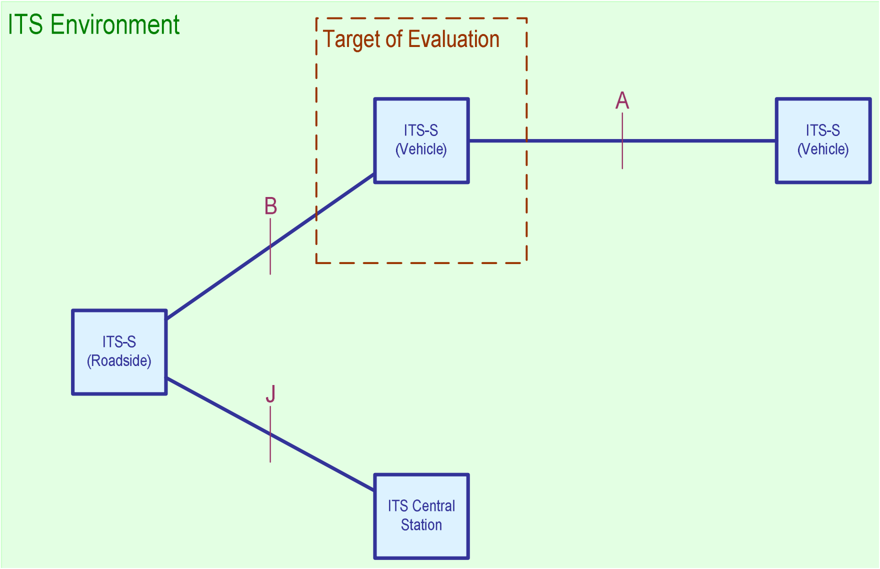

Figure 1: ITS-S (Vehicle) as the TOE

In the ITS-S (Roadside) case (Figure 2), only the interface at B is exposed and the ToE environment includes all ITS-S (Vehicle) units within range at any given point in time. This means that only the assets associated with the ITS-S (Vehicle) are potential threat agents or can be used as attack proxies. Although the interface at J is also exposed, it represents a fixed (rather than ITS G5A) connection to the ITS network infrastructure and it is assumed that this is secured by the ITS operator.

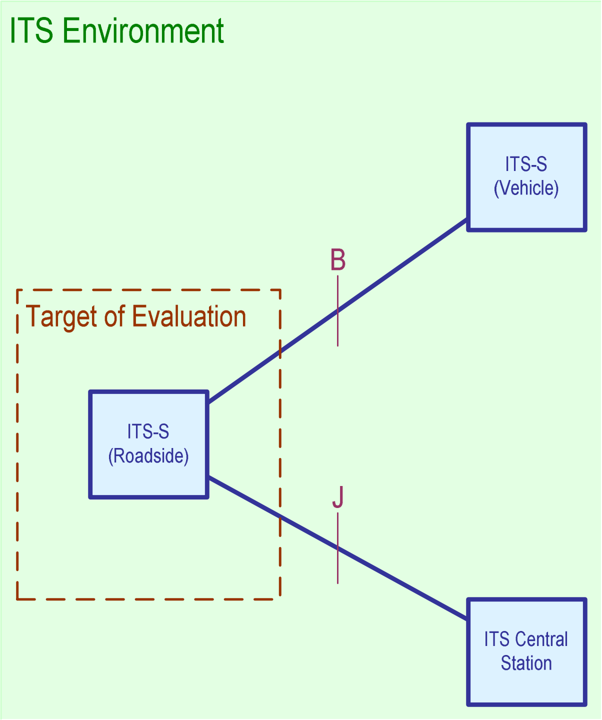

Figure 2: ITS-S (Roadside) as the TOE

8.2 Assumptions on the ToE

The following assumptions have been made for the purposes of this TVRA:

1) The ITS-S (Vehicle) and ITS-S (Roadside) are two distinct functional units although, in practice, they may be manufactured as a single physical device comprising both functionalities.

2) All communication and actions within the ToE are performed within the boundaries of a trust domain and are, therefore, secure.

3) ITS services are those defined in the ITS BSA [i.3].

4) All ITS stations have access to 5,9 GHz spectrum for sending.

5) All ITS stations have access to 5,9 GHz spectrum for receiving.

6) All ITS stations have the ability to determine trustworthiness of received information (i.e. the correctness of information).

7) All vehicles always know on which logical channel safety messages should be sent and received at any given point in time.

8) Restricted station data is only transmitted to authorized parties. Consequently, an ITS station needs to have the ability to validate the identity and authority of the recipient before sending restricted data.

8.3 Assumptions on the ToE environment

The following assumptions on the ToE environment have been made for the purposes of this TVRA:

1) The ITS network is not completely resistant to masquerade attacks and as a result attacks against ITS stations may originate from within the ITS network.

2) Communication over the interfaces at reference points J and K are considered to be secure.

3) There is no 5,9 GHz communication between two ITS-S (Roadside) units or between the ITS network and one or more ITS-S (Roadside) units.

4) There is no 5,9 GHz communication between the ITS network and an ITS-S (Vehicle).

5) Although it is possible that a physical and direct interface may exist at reference point K (for example, a maintenance access point directly connected to the vehicle at a service centre), it is also possible for K to be coincident with reference point B. Consequently, application and security parameter updates to ITS-S (Vehicle) can be made either directly over the fixed interface at K or indirectly over the ITS G5A interface at B (coincident with K).

6) All communication directly over the interfaces at K and J is secure.

7) Broadcast messages are not protected and assumed always to carry non-sensitive information (and as a consequence never carries personal data).

8) All communication between an ITS station and an end-user are considered to be part of a single trusted domain and, thus, out of scope of the TVRA.

9 ITS system assets

9.1 ITS station functional models

Two similar functional entities exist within the ITS 5,9 GHz model. These are the ITS Station (ITS-S) associated with a vehicle and the ITS-S associated with a roadside unit. Both of these can be represented by a number of functional and data elements (assets) as shown in Figure 3 and Figure 4. The assets shown are only those required to provide ITS services. Other security-specific assets are identified in the ITS threat analysis (clause 10).

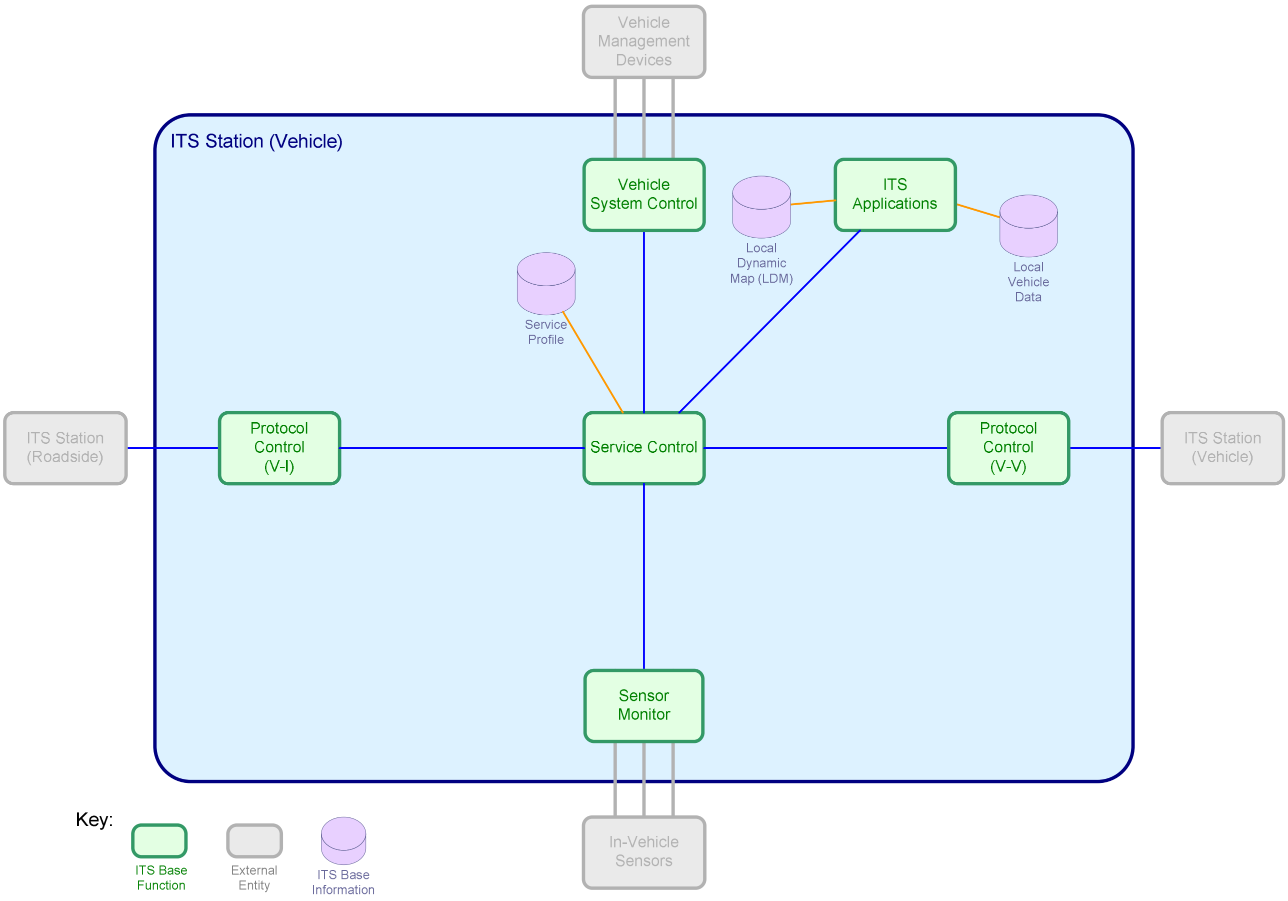

Figure 3: In-vehicle ITS Station assets

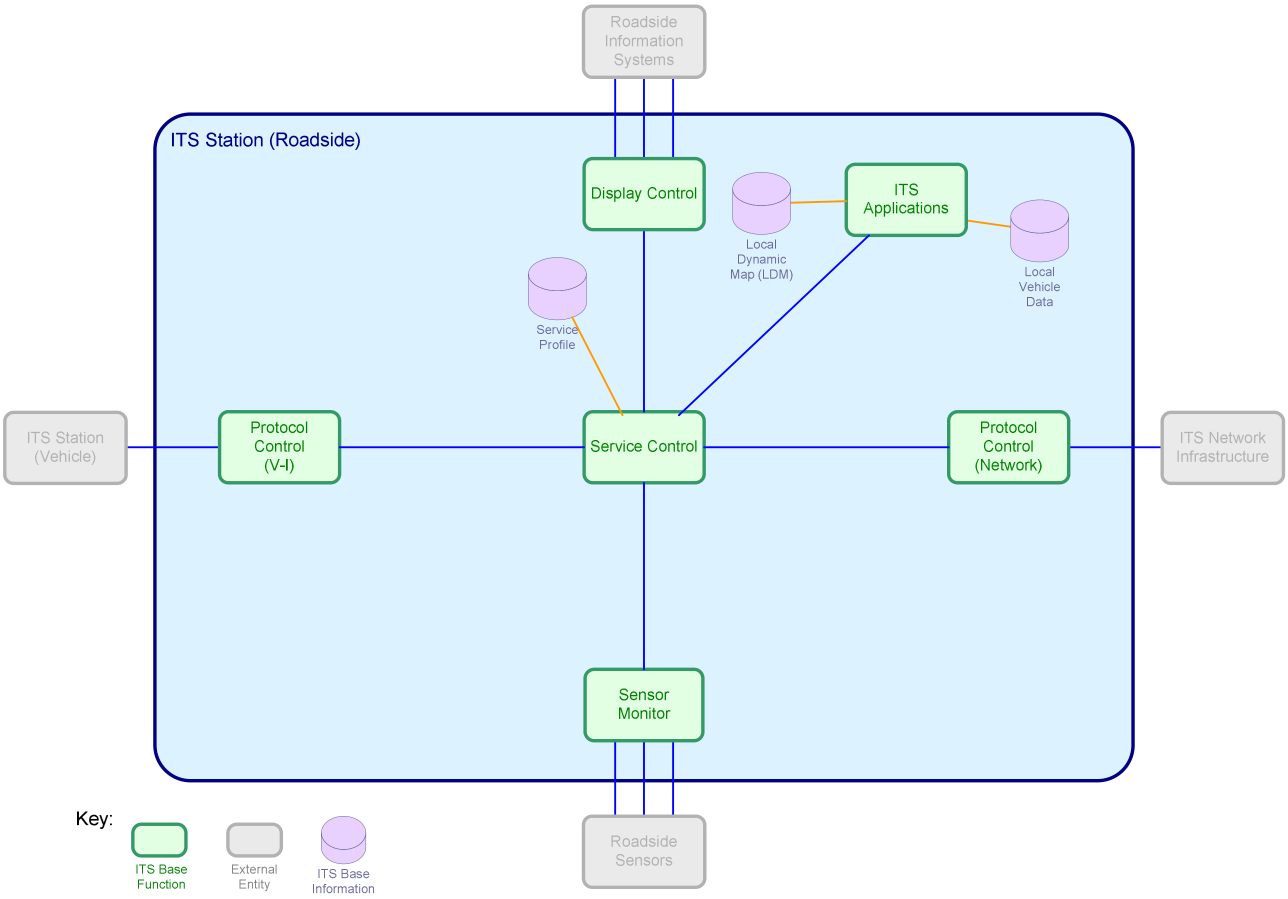

Figure 4: Roadside ITS station assets

9.2 Functional assets

9.2.1 ITS-S (Vehicle)

9.2.1.0 General

The functional assets that provide the base ITS capabilities in an in-vehicle ITS station include:

- protocol control:
  - vehicle to ITS infrastructure;
  - vehicle to vehicle;
- ITS applications;
- service control;
- on-board Sensor Monitor; and
- vehicle system control.

9.2.1.1 Protocol Control

9.2.1.1.1 General description

The protocol control assets select an appropriate message transfer protocol for an outgoing message request and sends the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the ITS station and passed to the relevant functional asset for further processing.

9.2.1.1.2 Vehicle to ITS infrastructure

The vehicle to ITS infrastructure (V2I) protocol control asset controls messages at reference point B between the vehicle and the ITS infrastructure.

9.2.1.1.3 Vehicle to vehicle

The vehicle to vehicle (V2V) protocol control asset controls messages at reference A between the vehicle and other vehicles.

9.2.1.2 Service Control

The Service Control functional asset enables information exchange between the other functional assets on the ITS station. It manages inter-process communications between those assets without altering the content of the communications. State information required to manage these communications, if it exists, is maintained and managed by Service Control and stored in the Service Profile data asset.

Service Control is responsible for invoking ITS applications and managing information about ITS application configuration, including:

- the list of applications installed and activated for transmission;
- the list of applications installed and activated for receipt;
- the list of applications installed and not activated.

This information is stored in the Service Profile.

Service Control may originate messages for transmission across the 5,9 GHz interface if those messages are necessary to maintain the Service Profile. However, no such instances have been identified in the ITS BSA.

9.2.1.3 ITS Applications

The ITS applications functional assets process ITS data for local use and determine when to initiate communications with other stations.

Examples of the functions that ITS applications may perform are:

- Maintaining information such as the Local Dynamic Map (LDM).
- Processing ITS-relevant information which may be received from both in-vehicle and external sources.
- Initiating actions including but not limited to:
    - notifying the driver or passengers of relevant information;
    - sending ITS messages to other parties;
    - passing commands through Service Control to request other functional assets to take direct action on the vehicle by, for example:
        - activating non-driving related vehicular components such as the air conditioning;
        - activating driving-related components such as the turn indicators;

    - reconfiguring the vehicle to reduce crash impact; and
    - taking direct driving actions such as steering, braking or accelerating.

Information is made available to the ITS applications via the Service Control functional asset. This information includes telematics data from the Sensor Monitor and Vehicle System Control and received ITS messages from the two Protocol Control assets.

An ITS application may originate messages for transmission across the 5,9 GHz interface in response to, for example:

- changes in the LDM;
- input from the Sensor Monitor; or
- decisions made by itself.

9.2.1.4 Sensor Monitor

The Sensor Monitor functional asset provides environmental data to Service Control for distribution to the other functional assets on the station. The environmental data provided may include:

- GNSS data;
- local telematics data such as current speed and bearing;
- external environmental data such as temperature, rain data and ambient light level;
- any ITS-relevant data other than the messages received over a 5,9 GHz wireless connection;
- human input received from a user interface.

Different vehicles will contain different implementations of the sensor monitor. Consequently, different Vehicle ITS Stations may have different collections of environmental data available to them.

The end-user of a vehicle may originate messages for transmission across the 5,9 GHz interface using the Sensor Monitor. However, no such instances have been identified in the ITS BSA.

9.2.1.5 Vehicle System Control

The Vehicle System Control functional asset allows other functional assets to access the vehicle control systems via Service Control. Access to the vehicle control systems allows the ITS-S to control vehicle behavior. Examples of this may include:

- providing information to the driver only, to the passengers only or to both driver and passengers;
- playing a sound;
- operating the air-conditioning/heating system;
- changing the volume on the car entertainment system;
- activating or deactivating voice communications;
- locking/unlocking/opening/closing doors;
- reconfiguring the vehicle to reduce the damage caused by an imminent collision;
- taking direct control of certain driving actuators.

Not all vehicles will support all of these operations, particularly in the early days of deployment of ITS. However, it is assumed that Vehicle System Control will have access to a Human-Machine Interface (HMI) component which it can use to provide pertinent notifications to the driver.

This FA also includes transmission of messages over interfaces other than the 5,9 GHz interface.

Vehicle System Control is assumed to implement all vehicle control requests from other functional assets without regard to the specific contents of those requests.

Although it is likely that Vehicle System Control will transmit messages over a range of internal interfaces, it should not originate messages for transmission over the 5,9 GHz interface.

9.2.2 ITS-S (Roadside)

9.2.2.0 General

The functional assets that provide the base ITS capabilities in a roadside ITS station include:

- Protocol Control:
  - RSU to vehicle;
  - RSU to ITS network.
- ITS Applications;
- Service Control;
- roadside Sensor Monitor; and
- roadside Display Control.

9.2.2.1 Protocol Control

9.2.2.1.1 General description

The Protocol Control assets select an appropriate message transfer protocol for an outgoing message request and sends the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the ITS station and passed to the relevant functional asset for further processing.

9.2.2.1.2 RSU to vehicle

The vehicle to ITS infrastructure (V2I) Protocol Control asset controls messages at reference point B between the roadside unit and vehicles.

9.2.2.1.3 RSU to ITS network

The vehicle to vehicle (V2V) protocol control asset controls messages at reference point J between the RSU and the ITS Service Centre.

The roadside-to-network interface will not be a 5,9 GHz connection and so attacks on the RSU using this interface are not considered in the analysis. However, it is conceivable that forged Service Centre messages could enter the RSU at this point and be forwarded to vehicles. This Protocol Control asset is, therefore, considered to be capable of originating messages to be passed across the 5,9 GHz interface.

9.2.2.2 Service Control

The Service Control functional asset enables information exchange between the other functional assets on the ITS station. It manages inter-process communications between those assets without altering the content of the communications. State information required to manage these communications, if it exists, is maintained and managed by Service Control and stored in the Service Profile data asset.

Service Control is responsible for invoking ITS applications and managing information about ITS application configuration, including:

- the list of applications installed and activated for transmission;
- the list of applications installed and activated for receipt;
- the list of applications installed and not activated.

This information is stored in the Service Profile.

Service Control may originate messages for transmission across the 5,9 GHz interface if those messages are necessary to maintain the Service Profile. However, no such instances have been identified in the ITS BSA.

9.2.2.3 ITS Applications

The ITS applications functional assets process ITS data for local use and determine when to initiate communications with other stations.

Examples of the functions that ITS applications may perform are:

- Maintaining information such as the Local Dynamic Map (LDM).
- Processing ITS-relevant information which may be received from both in-vehicle and external sources.
- Initiating actions including but not limited to:
  - sending ITS messages to other parties;
  - sending information to the Display Control asset to be presented on roadside matrix units;
  - sending information to the ITS Service Centre.

Information is made available to the ITS applications via the Service Control functional asset. This information includes telematics data from the Sensor Monitor and Vehicle System Control and received ITS messages from the two Protocol Control assets.

An ITS application may originate messages for transmission across the 5,9 GHz interface in response to, for example:

- changes in the LDM;
- input from the Sensor Monitor; or
- decisions made by itself.

9.2.2.4 Sensor Monitor

The Sensor Monitor functional asset provides environmental data to Service Control for distribution to the other functional assets on the station. The environmental data provided may include:

- GNSS data;
- external environmental data such as temperature, rain data and ambient light level;
- any ITS-relevant data other than the messages received over a 5,9 GHz wireless connection;
- human input received from a user interface.

Different vehicles will contain different implementations of the sensor monitor. Consequently, different Roadside ITS Stations may have different collections of environmental data available to them.

The end-user of an RSU may originate messages for transmission across the 5,9 GHz interface using the Sensor Monitor. However, no such instances have been identified in the ITS BSA.

9.2.2.5 Display Control

The Display Control functional asset manages the information sent to external presentation devices such as electronic road signs and smaller displays intended for use by a human operator. Data Control may be used by the ITS Applications, the ITS network via the ITS Network Protocol Control, a human operator via the Sensor Monitor FA and Service Control. When requested to display a message, Display Control will pass the information to the presentation device without regard to the contents of the message.

Display Control does not originate message for transmission over the 5,9 GHz interface.

9.3 Data assets

9.3.1 ITS-S (Vehicle)

9.3.1.1 Local Dynamic Map

The Local Dynamic Map (LDM) is an in-vehicle ITS station's dynamically updated repository of data relating to local driving conditions. It includes information received from on-board sensors and from CAM and DNM messages.

Data from sensors includes the following:

- vehicle's current position;
- data that has been made public regarding the vehicle's current status. For example:
  - braking information;
  - traction information;
  - status of external indicators;
- data that has not yet been made public regarding the vehicle's current status but might be in the future. For example:
  - tyre tread state;
- data that will not be shared regarding the vehicle's current status but which is relevant to driving decisions. For example:
  - amount of fuel remaining;
  - current fuel consumption.

Data resulting from received messages includes the following:

- current known positions and types of other vehicles;
- current hazards, alerts, and other DNM-related information.

Some data may be updated as a result of either sensor input or received messages, such as:

- local weather conditions;
- local road surface conditions;
- other information about the physical (as opposed to simply ITS) environment.

9.3.1.2 Local Vehicle Information

Local vehicle information comprises data relating to the vehicle that may not be immediately relevant to real-time driving decisions but may be used for maintenance or may influence driving strategy. There is an overlap between this information and the "data that will not be shared" in the LDM. Although there is no definitive list of what might be included in the Local Vehicle Information repository, the following items are potential candidates:

- Vehicle Identification Number (VIN);
- license plate number;
- vehicle manufacturer;
- model of vehicle;
- known physical damage;
- inventory of components on the vehicle:
  - component manufacturer;
  - date of manufacture.

Additionally, an owner may store personal information on the vehicle (this is not required for any of the ITS applications in the BSA but, again, may facilitate obvious next-generation applications). This information would generally relate to the owner or operator of the vehicle and may include:

- name;
- address;
- telephone number;
- credit card number (to allow on-road e-commerce);
- toll road subscriber identity.

9.3.1.3 Service Profile

A service profile in an in-vehicle ITS station will include:

- the list of applications installed and activated for transmission;
- the list of applications installed and activated for receipt;
- the list of applications installed and not activated.

In addition, references to specific security parameters and other characterization data may be stored for each application.

NOTE: The term "application" may not map exactly to an application in the sense of CAM or DNM. An application here is a set of messages that the vehicle is permitted to send or is willing to receive. These messages may be a subset of the CAM or DNM messages or they may be other messages entirely from outside the BSA.

9.3.2 ITS-S (Roadside)

9.3.2.1 Local Dynamic Map (LDM)

The Local Dynamic Map (LDM) is a roadside ITS station's dynamically updated repository of data relating to local driving conditions. It includes information received from roadside sensors, the ITS infrastructure network and from CAM and DNM messages.

Data acquired from sensors or received from the ITS infrastructure network includes the following:

- current position.

Data resulting from messages received from other vehicles includes the following:

- current known positions and types of other vehicles.

Some data may be updated as a result of input over either 5,9 GHz or non-5,9 GHz interfaces, such as:

- local weather conditions;
- local road surface conditions;
- other information about the physical (as opposed to simply ITS) environment;
- current hazards, alerts, and other DNM-type information.

9.3.2.2 Local Station Information

Local station information contains information about the RSU that may be relevant for service management. This category includes the following:

- RSU serial number;
- networking information;
- current operational status of the RSU;
- ITS operator;
- maintenance schedule.

9.3.2.3 Service Profile

The service profile in an RSU ITS station includes:

- the list of applications installed and activated for transmission;
- the list of applications installed and activated for receipt;
- the list of applications installed and not activated.

In addition, references to specific security parameters and other characterization data may be stored for each application.

NOTE: The term "application" may not map exactly to an application in the sense of CAM or DNM. An application here is a set of messages that the RSU is permitted to send or is willing to receive. These messages may be a subset of the CAM or DNM messages or they may be other messages entirely from outside the BSA.

10 ITS threat analysis

10.1 Attack interfaces and threat agents

10.1.1 Attack interfaces and threat agents for ITS-S (Vehicle) ToE

The ITS-S (Vehicle) ToE accesses its environment across ITS G5A interfaces at the three reference points A, B and K (coincident with B). These interfaces are all exposed which means that they are accessible from outside of the ToE and may, therefore, be exploited as attack interfaces.

The interface at reference point A can be exploited as an attack interface by another valid ITS-S (Vehicle) causing undesired actions or events due to, for example:

- design flaws as a result of poorly specified requirements;
- malicious or mischievous use of an ITS-S (Vehicle) as an attack proxy by a remote agent; or
- malicious or mischievous use as an ITS-S (Vehicle) providing false or misleading information to other vehicles.

The interface at reference point B can be exploited as an attack interface by a valid ITS-S (Roadside) unit causing undesired actions or events due to, for example:

- design flaws as a result of poorly specified requirements;
- malicious or mischievous use as an attack proxy by a remote agent; or
- malicious or mischievous use as an ITS-S (Roadside) providing false or misleading information to passing vehicles.

The interface at reference point K cannot be directly exploited when it is implemented as a wired and controlled interface. However, it can be exploited as an attack interface when coincident with reference point B implemented as a 5,9 GHz interface. In this case it is possible for an attack on an ITS-S (Vehicles) to be mounted from the ITS network.

Any security attack can in principle originate from any logical entity in the ToE environment and may target any of the assets of a target ITS-S (Vehicle). Furthermore, any layer in the protocol stack used by the relevant reference point can be exploited as an attack interface.

10.1.2 Attack interfaces and threat agents for ITS-S (Roadside) ToE

The ITS-S Roadside unit accesses its environment across the ITS G5A interface at reference point B. This interface is exposed and may, therefore, be exploited as an attack interface into the ToE. Attacks originate either from within the ToE environment or from within the ToE itself. Roadside units communicates with each other through the ITS core network without using 5,9 GHz communication links. However, the interface at reference point J between the ITS-S roadside unit and the ITS network can be used to carry an attack, such as the installation of malware, from the ITS network. This interface is, therefore, also defined as an exposed interface of the ITS-S (Roadside) unit.

The interface at reference point B can be used by a number of threat agents in order to mount an attack. These threat agents may include:

- a valid ITS-S (Vehicle) causing undesired actions or events due to, for example:
  - design flaws as a result of poorly specified requirements;
  - malicious or mischievous use as an attack proxy by a remote agent; or
  - malicious or mischievous use as an ITS-S (Vehicle) providing false or misleading information to other vehicles;
- an entity posing as a valid ITS-S (Vehicle) causing undesired actions or events due to, for example:
  - malicious or mischievous use as an attack proxy by a remote agent; or
  - malicious or mischievous use as an ITS-S (Vehicle) providing false or misleading information to other vehicles;
- an entity within the ITS-S (Roadside) itself providing false or misleading information to passing vehicles.

When an attack originates from within the roadside unit, the interface at B may be used to propagate the attack into the ToE environment.

The interface at reference point J is not expected to be an ITS G5A interface and assumed to be secured against direct attack. However, it can be used to carry an accidental or malicious attack from within the ITS network.

Any security attack on an ITS-S (Roadside) ToE could originate in any logical entity in the ToE environment and may target any of the assets of a target ITS-S (Roadside). Furthermore, any layer in the protocol stack can be exploited as an attack interface.

10.2 Vulnerabilities and threats

10.2.1 Threats to all ITS stations

The identification and analysis of ITS security considered threats in the following categories:

- Availability threats:
  - Denial of Service (DoS).
- Integrity threats:
  - Manipulation.
  - Masquerade.
  - Replay.
  - Insertion of information.
- Authenticity threats:
  - Manipulation.
  - Masquerade.
- Confidentiality threats:
  - Eavesdropping.
  - Traffic analysis.
- Non-repudiation/Accountability threats:
  - Repudiation.

10.2.2 Availability

10.2.2.1 General threats to availability

Threats to the availability and continuous behavior of an ITS system include Denial of Service (DoS) attacks as a result of, for example:

- the introduction of malicious software (malware);
- a high volume of messages introduced intentionally through spamming; and
- a high volume of messages introduced as a consequence of using multi-hop broadcast messaging:
  - this may pose a threat to the system because time is a critical component in traffic safety messages and the design of an ITS-S may not allow sufficient time to check for the authenticity of relay messages when large numbers are received in a very short time.

DoS is a category of attack that is difficult to protect against. Such attacks may results in an ITS station failing to receive, respond to, relay, produce and send traffic safety messages or to perform its normal function or prevent other ITS stations from performing their normal functions. Methods of attack include:

- maliciously and artificially generating a high volume of false messages;

- malware manipulating the sending or receiving capabilities of an ITS station. Injecting malware is made possible by exploiting the capability of an ITS-S to receive periodic software and firmware updates and security parameter information updates;
- formation of "black holes" when a number of adjacent ITS stations are configured (either accidentally or maliciously) not to propagate messages. The impact of having a black hole is that ITS messages are not relayed to all users in a target area. There is also the possibility that an ITS-S (Vehicle) may be manipulated such that when it enters a particular area (given by GNSS coordinates) it stops relaying messages. Such an attack creates a vehicle local "black hole" at a particular location;
- accidentally generating a high volume of false outgoing messages or unsolicited incoming message queue entries as a result of flaws in the product design.

10.2.3 Integrity

10.2.3.1 General threats to integrity

Threats to the integrity of an ITS-S include:

- unauthorized access to restricted information;
- loss of information;
- manipulation of information; and
- corruption of information.

Unauthorized access to restricted information can be gained by means of a masquerade attack or by the use of malware injected into an ITS station. Restricted information includes all information which would not be included in broadcast messages and which is specifically associated with a particular ITS station or its end-users.

Loss of information can be a consequence of unauthorized access to restricted information. An attacker could insert malware that deletes service information, security parameters, local station data or information stored in the LDM.

Information can be manipulated or corrupted either at one of the ITS G5A interfaces or within the sending and receiving ITS stations. Malware could be used to change a message before it is sent or to interfere with the protocol such that information is corrupted in transit.

10.2.4 Authenticity

10.2.4.1 General threats to authenticity

Authenticity is a major security challenge in ITS as all ITS stations have the ability to send, receive and replay all types of messages defined in the BSA except those which are specific to emergency vehicles.

Ensuring the authenticity of information received and processed by an ITS-S involves some or all of the following:

- Protection of legitimate ITS stations from masquerade attacks:
    - Carried out by an agent posing as a legitimate ITS station, application or service. An attacker can then insert false messages into the network and deceive users and authorities into believing that another node was responsible for sending these messages.
- Identification of the unplanned replay of previous legitimate message interchanges:
    - Carried out by capturing and subsequently resending valid received messages. Replay attacks can take two general forms:
        - replay of messages at a similar location but a different time. Such attacks would include the replay of emergency vehicle messages when the specific emergency situation no longer exists;

    - replay of messages at a different location and a different time, the so called "wormhole attack". Such attacks can be used to cause confusion among recipients who are unable to resolve the received location data with their own actual location and may, consequently, send messages which could reveal their identity or other private information.

- Exposure of false GNSS signals:
  - A GNSS satellite simulator can generate radio signals that are stronger than those received from a genuine GNSS satellite. This enables an attacker to provide false location information to ITS stations and thus, potentially, causing traffic accidents. If an ITS-S synchronizes its internal clock to GNSS time, a simulator can be used to set an inaccurate current time and this can result in it accepting expired messages received in a replay attack.
- Protection against broadcast messages carrying misinformation (Illusion attack [i.11]):
  - Carried out by broadcasting valid but false ITS messages in order to misinform the message recipients. The motivation for this attack may be to clear a chosen route for personal or criminal purposes.
- Protection against multiplication of fake nodes (Sybil attack [i.11]):
  - Carried out by sending multiple messages from one node with multiple identities. it consists on giving receivers applications false information about the neighbors' density and behaviors. The main motivation of this attacks is to gain advantage on road.

10.2.5 Confidentiality

10.2.5.1 General threats to confidentiality

Threats to the confidentiality of information associated with an ITS station include the illicit collection of transaction data by eavesdropping and the collection of location information through the analysis of message traffic.

The messages associated with the BSA services considered in this analysis are those transmitted over the 5,9 GHz radio interface. As G5A is an open interface, messages transmitted over this interface may be intercepted and information extracted. Information that is of particular concern in this context includes personal data and data that can later be used to launch a direct attack (replay, for example). ITS broadcast messages are transmitted indiscriminately and so can be received by any ITS-S within range of the radio signal. Consequently, these messages are of little interest to an eavesdropper.

An attacker may also construct a profile of a given ITS-S (Vehicle) or end-user by observing which services are used regularly, at what times and at which location. Such traffic analysis might be used to gain information on private vehicles which are used as emergency vehicles thus enabling the attacker to carry out an emergency vehicle masquerade attack.

The ITS system requirement of being able to track vehicles for traffic flow and safety purposes can be misused by an attacker to gain information about the whereabouts of a particular vehicle. In this way, the attacker is able to stalk the user or build a profile of the ITS station for potentially malicious purposes.

10.2.6 General threats to accountability

ITS end-users may be able to avoid prosecution for motoring offences or for mounting security attacks on other ITS users by denying that:

- particular ITS messages were sent by an ITS station;
- particular ITS messages were received by an ITS station;
- specific ITS services were uploaded, deleted or otherwise modified;
- specific ITS data were uploaded, deleted or otherwise modified.

For law enforcement authorities to be able to prosecute such actions, it is necessary to record all message and service activity within the an ITS station.

10.2.7 Vulnerabilities and threats

10.2.7.1 Determining system vulnerabilities

Within a ToE, a vulnerability is considered to be a combination of an identified system weakness with one or more threats that are able to exploit that weakness.

10.2.7.2 Threats and vulnerabilities within an ITS-S (Vehicle)

Table 8 identifies the threats and associated weaknesses that define the vulnerabilities within an ITS-S (Vehicle).

Table 8: List of Vulnerabilities for ITS-S (Vehicle) ToE

ID	Threat	ITS-S Problem Area	Weaknesses	Threat Agent	Attack interface
V-V1	- Message saturation	Intrinsic high density of ITS message traffic due to broadcasting and beaconing in V2V systems	The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages or fabricated queue entries could: (1) cause it to miss important incoming ITS messages (2) cause it to delay or miss the sending of outgoing ITS messages or relaying of incoming ITS messages (3) leave it with no resources free for other essential tasks such as monitoring sensors and updating driver-displays (4) leave it with no resources free for other essential tasks such as monitoring sensors and updating driver-displays	Malware installed on target ITS-S (Vehicle) filling the incoming message queue with spurious but valid messages Malicious ITS-S broadcasting a high level of ITS message traffic	A, B (also on behalf of K)
		Lack of flow control in V2V broadcast messaging			
		Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected by the application, not at the network layer in the ITS stack			
		The random re-attempt period in the "Listen before send" message transmission method does not make optimum use of the available bandwidth			

ID	Threat	ITS-S Problem Area	Weaknesses	Threat Agent	Attack interface
V-V2	- Jamming of radio signals	Inability of the ITS-S (Vehicle) to quickly detect and isolate interference on radio channels	Transmissions to and from an ITS-S (Vehicle) can be lost while interference is detected and mitigated	External jammer equipment	A, B
V-V3	- Injection of false messages - Manipulation of ITS messages en route	Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected at the application layer, not at the network layer in the ITS stack	An ITS-S (Vehicle) is unable to determine quickly whether a received message is valid and from a legitimate user and then acts on information received in the message Relayed messages are open to manipulation in an ITS-S en route. Received messages that are intended for relaying can be withheld	Malware on ITS-S (Vehicle or Roadside) within range Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending valid but irrelevant ITS messages	A, B
V-V4	- Masquerade as ITS-S (Vehicle or Roadside) or ITS network	CAM and DNM messages do not include any form of identification information	An ITS-S (Vehicle) is unable to determine quickly whether a received message is valid and from a legitimate user and then acts on information received in the message The contents of the LDM can be incorrectly modified by received messages containing false time, position or status information or by maliciously planted software	Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending false information in ITS messages that are otherwise valid	A, B (also on behalf of K)
		Vehicle-to-Vehicle messages include no validation or legitimacy checks			
V-V5	- Masquerade for fabrication of messages	CAM and DNM messages do not include any form of identification information	An ITS-S (Vehicle) is able to perform only basic checks on the validity of a received message and its contents The contents of the LDM can be incorrectly modified by received messages containing false time, position or status information or by maliciously planted software	Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending false information in ITS messages that are otherwise valid Malicious application in the ITS network sending false information in ITS messages that are otherwise valid	A, B
		Vehicle-to-Vehicle messages include no validation or legitimacy checks			

ID	Threat	ITS-S Problem Area	Weaknesses	Threat Agent	Attack interface
V-V6	- Replay of "expired" (old) messages - Wormhole attacks - GNSS spoofing	Uncertainty regarding how timestamps are created and how to use them to check the validity of messages	An ITS-S (Vehicle) is unable to validate when or where a received message was originally generated	Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending "expired" information in ITS messages that are otherwise valid Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending information in ITS messages that are valid except for the source location	A, B
V-V7	- Malicious isolation of one or more ITS-S (Vehicle) (black hole)	ITS-S (Vehicle) memory is can be modified by information received over the air interface	Malware can be initiated, accessed or installed over the air	Malware on ITS stations that disables some or all functionality of one or more of the ability to create, process, receive and send ITS messages	A, B
V-V8	- Eavesdropping - Traffic analysis - Location tracking	Broadcast messages are in general intended for all ITS-S within range.	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver Some ITS BSA messages reveal the geographic location of the sending ITS-S	Equipment posing as a genuine ITS-S (Vehicle) or as an RSU receiving information for malicious analysis of content and recording on message patterns, etc.	A, B
		Absence of addressing in broadcast messages meaning that non-ITS-S equipment can also receive ITS messages			

ID	Threat	ITS-S Problem Area	Weaknesses	Threat Agent	Attack interface
V-V9	- Denial of transmission	CAM and DNM messages do not include any form of identification information	There is no requirement for an ITS-S (Vehicle) to maintain an auditable log of all messages sent and received by it. Such a log would quickly become very large due to the high density of ITS messages.	Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending false information in ITS messages that are otherwise valid Malware installed on target ITS-S (Vehicle) creating and sending false information in ITS messages that are otherwise valid	A, B (also on behalf of K)
		Vehicle-to-Vehicle messages include no validation or legitimacy checks			
		ITS-S (Vehicle) cannot positively identify relevant information to maintain record of the originator of ITS messages causing harm to the ITS-S (Vehicle)			

A successful attack on each vulnerability in an ITS-S (Vehicle) may result in a number of undesirable consequences. These are listed in Table 9 to Table 13.

Table 9: Consequences of threats to availability in an ITS-S (Vehicle)

Threat Group		Threat Type	Weakness	Undesirable Consequences
DoS:	Denial of access to incoming messages	- Message saturation - Radio jamming - Injection of false messages - Internal malware	An ITS-S (Vehicle) is unable to quickly determine whether a received message is valid and from a legitimate user and acts on information received in the message The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages could cause it to miss important incoming ITS messages	Accidents if collision warnings are not received and processed by the attacked ITS-S (Vehicle) General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages
DoS	Denial of access to outgoing messages	- Message saturation - Radio jamming - Internal malware - Black hole creation	The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages or fabricated queue entries could cause it to delay or miss the sending of outgoing ITS messages or relaying of incoming ITS messages Transmissions to and from an ITS-S (Vehicle) can be lost while interference is detected and mitigated	Accidents if collision warnings are not delivered by the attacked ITS-S (Vehicle) General compromise of traffic management applications which depend on the reliable and timely delivery of ITS messages to all affected vehicles
DoS	Denial of access to ITS-S (Vehicle) internal resources	- Message saturation - Internal malware	The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages or fabricated queue entries could leave it with no resources free for other essential tasks such as monitoring sensors and updating driver-displays	Accidents if driver is not warned immediately of critical events or significant environmental changes General compromise of traffic management applications which depend on the reliable and timely processing of changes in vehicle and ITS-S (Vehicle) environment status

Table 10: Consequences of threats to integrity in an ITS-S (Vehicle)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Modification and deletion of stored information	- Internal malware - Message replay - GNSS spoofing - ITS-S masquerade - Injection of false ITS messages	An ITS-S (Vehicle) is unable to validate when a received message was originally generated The contents of the LDM can be incorrectly modified by received messages containing false time, position or status information or by maliciously planted software	General compromise of traffic management applications which depend on the LDM for accurate and up-to-date information
Modification and deletion of transmitted information	- Relay modification - Black hole	Relayed messages are open to manipulation in an ITS-S en route. Received messages that are intended for relaying can be withheld. An ITS-S (Vehicle) is unable to determine quickly whether a received message is valid and from a legitimate user and then acts on information received in the message	Accidents if collision warnings are not received and processed by the attacked ITS-S General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages

Table 11: Consequences of threats to authenticity in an ITS-S (Vehicle)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Masquerade	- Emergency vehicle masquerade - Message replay - Wormhole attack - GNSS spoofing - ITS-S masquerade - Injection of false ITS messages - Sybil attack	An ITS-S (Vehicle) is able to perform only basic checks on the validity of a received message and its contents	Accidents and general driver confusion if the source and contents of received messages cannot be relied upon General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages

Table 12: Consequences of threats to confidentiality in an ITS-S (Vehicle)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Acquisition of personal information	- Eavesdropping	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver	Without protection, any personal information exchanged in a unicast transaction could be intercepted and used by an attacker to gain illicit access to subscription services
Acquisition of behavioral details	- Eavesdropping - Traffic analysis	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver	Analysis of message traffic can reveal which subscription services are being used by individual users. This information can be used to launch direct attacks on a particular ITS-S (Vehicle) and user
Acquisition of location information	- Traffic analysis - Location tracking	Some ITS BSA messages reveal the geographic location of the sending ITS-S	Location information gained in an unauthorized way can be used to effectively launch other directed attacks against particular ITS-S (Vehicle)s and users

Table 13: Consequences of threats to accountability in an ITS-S (Vehicle)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Denial of transmission	- Repudiation	There is no requirement for an ITS-S (Vehicle) to maintain an auditable log of all messages sent by it. Such a log would quickly become very large due to the high density of ITS messages	Malicious and mischievous messages can be sent with impunity by a legitimate ITS-S (Vehicle) as no proof exists that any particular message was ever sent by that particular ITS-S
Denial of data receipt	- Repudiation	There is no requirement for an ITS-S (Vehicle) to maintain an auditable log of all messages received by it. Such a log would quickly become very large due to the high density of ITS messages	Traffic safety and traffic management messages can be ignored so that, in the event of prosecution (for a speeding offence, for example), a vehicle owner can claim that the message was not received

10.2.7.3 Threats and vulnerabilities within an ITS-S (Roadside)

Table 14 identifies the threats and associated weaknesses that define the vulnerabilities within an ITS-S (Roadside).

Table 14: List of Vulnerabilities for ITS-S (Roadside)

ID	Threat	ITS-S Problem Area	Weakness	Threat Agent	Attack interface
V-R1	- Injection of a high volume of false emergency vehicle warning messages	CAM and DNM messages do not include any form of identification information Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected on the application layer, not at the network layer in the ITS stack	An RSU is unable to quickly determine whether a received message contains accurate information and is from a legitimate emergency services vehicle and acts by relaying the message. An RSU can only check whether the message is valid and comes from a valid source The time taken by an RSU to process a high volume of real or spurious messages could cause it to miss important incoming ITS messages	Equipment posing as a genuine Emergency Vehicle sending false information in ITS messages that are otherwise valid Equipment replaying "expired" emergency vehicle warnings	B
V-R2	- Message saturation	CAM and DNM messages do not include any form of identification information Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected on the application layer, not at the network layer in the ITS stack Uncertainty regarding identification, authentication and authorization of ITS application and information on an RSU	The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages or fabricated queue entries could cause it to miss important incoming ITS messages The time taken by an RSU to process a high volume of real or spurious messages or fabricated queue entries could leave it with no resources free for other essential tasks such as relaying and acting upon emergency vehicle warnings or other safety-related messages	Malware installed on target RSU filling the incoming message queue with spurious but valid messages Malicious ITS-S broadcasting a high level of ITS message traffic	B
V-R3	- Radio jamming	Inability of an RSU to quickly detect and isolate interference on radio channels	Transmissions to and from an RSU can be lost while interference is detected and mitigated	External jammer equipment	B

ID	Threat	ITS-S Problem Area	Weakness	Threat Agent	Attack interface
V-R4	- Injection of false messages	Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected on the application layer, not at the network layer in the ITS stack Uncertainty regarding how timestamps are created and how to use them to heck the validity of messages	An RSU is unable to quickly determine whether a received message contains accurate information and is from a legitimate user and acts by relaying the message. An RSU can only check whether the message is valid and comes from a valid source The time taken by an RSU to process a high volume of real or spurious messages could cause it to miss important incoming ITS messages An RSU is unable to validate when a received message was originally generated	Equipment posing as a genuine ITS-S (Vehicle) sending false information in ITS messages that are otherwise valid	B
V-R5	- Replay of "expired" (old) messages - Wormhole attack - GNSS spoofing	Uncertainty regarding how timestamps are created and how to use them to heck the validity of messages	An RSU is unable to validate when a received message was originally generated	Equipment posing as a genuine ITS-S sending "expired" information in ITS messages that are otherwise valid GNSS spoofing equipment	B
V-R6	- Emergency vehicle masquerade	CAM and DNM messages do not include any form of identification information Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected on the application layer, not at the network layer in the ITS stack	An RSU is unable to quickly determine whether a received message contains accurate information and is from a legitimate emergency services vehicle and acts by relaying the message. An RSU can only check whether the message is valid and comes from a valid source	ITS-S masquerading as Emergency Vehicle Equipment posing as a genuine Emergency Vehicle	B
V-R7	- Eavesdropping - Traffic analysis - Location tracking	Broadcast messages are in general intended for all ITS-S within range Absence of addressing in broadcast messages meaning that non-ITS-S equipment can also receive ITS messages	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver Some ITS BSA messages reveal the geographic location of the sending ITS-S	Equipment posing as a genuine ITS-S (Vehicle) or RSU recording information in ITS messages for malicious analysis of content, behavioral patterns, etc.	B, J

ID	Threat	ITS-S Problem Area	Weakness	Threat Agent	Attack interface
V-R8	- Transaction tampering	Broadcast messages are in general intended for all ITS-S within range	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver An RSU is unable to validate either when a received message was originally generated or whether any subscription information in the messages is valid	Equipment posing as a valid ITS-S (Vehicle)	B
		Absence of addressing in broadcast messages meaning that non-ITS-S equipment can also receive ITS messages			
		Uncertainty regarding how timestamps are created and how to use them to heck the validity of messages			
V-R9	- Denial of transmission	CAM and DNM messages do not include any form of identification information	There is no requirement for an RSU to maintain an auditable log of all and specific types of messages sent and received by it. Such a log should be maintainable for an RSU	Equipment posing as a genuine RSU or ITS-S (Vehicle) sending false information in ITS messages that are otherwise valid Malware installed on target RSU creating and sending false information in ITS messages that are otherwise valid Valid ITS-S (Vehicle) with motivation to deny sending or receiving ITS messages, such as ITS messages from authorities	B, J
		RSU cannot positively identify relevant information to maintain record of the originator of ITS messages causing harm to the RSU			

A successful attack on each vulnerability in an ITS-S (Roadside) may result in a number of undesirable consequences. These are listed in Table 15 to Table 19.

Table 15: Consequences of threats to availability in an ITS-S (Roadside)

Threat Group	Threat Type	Weakness	Undesirable Consequences
DoS: Forgery of emergency vehicle warning message	- Injection of high volume of false emergency vehicle warning messages	An RSU is unable to unable to validate either the accuracy of the contents of a message or whether it originated in a vehicle authorized to send emergency vehicle warning message and, so, relays the message An RSU can only check whether the message is valid and comes from a valid source The time taken by an RSU to process a high volume of real or spurious messages could cause it to miss important incoming ITS messages	Temporary blocking of emergency vehicle warning message from a particular originator if RSU discover that similar messages are sent from multiple locations Accidents due to general driver confusion Delay of actual emergency vehicle warning messages
DoS: Denial of access to incoming messages	- Message saturation - Radio jamming - Injection of false messages - Internal malware	An RSU is unable to unable to validate either the accuracy of the contents of a message or whether it originated in a vehicle authorized to send emergency vehicle warning message and, so, relays the message An RSU can only check whether the message is valid and comes from a valid source Transmissions to and from an RSU can be lost while interference is detected and mitigated The time taken by an RSU to process a high volume of real or spurious messages could cause it to miss important incoming ITS messages	Accidents if collision warnings are not received and processed by the attacked RSU General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages

Table 16: Consequences of threats to integrity in an ITS-S (Roadside)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Modification and deletion of transmitted information	- Transaction tampering - Internal malware - Replay of "expired" (old) messages - GNSS spoofing	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver An RSU is unable to validate when a received message was originally generated or if any subscription information in the messages is valid	Vehicles within range of the ITS-S (Roadside) receive and install compromised or illicit services Vehicles within range of the ITS-S (Roadside) are denied access to subscribed services
Masquerade as emergency vehicle	- Forgery of emergency vehicle warning message	An RSU is unable to unable to validate either the accuracy of the contents of a message or whether it originated in a vehicle authorized to send emergency vehicle warning message	General driver confusion upon reception of false emergency vehicle warning. Accident may happen as a consequence of several vehicles adjusting their driving to give way to a non-existing emergency vehicle

Table 17: Consequences of threats to authenticity in an ITS-S (Roadside)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Masquerade	- Emergency vehicle masquerade - Masquerade	An RSU is unable to unable to validate either the accuracy of the contents of a message or whether it originated in a vehicle authorized to send emergency vehicle warning message and, so, relays the message An RSU can only check whether the message is valid and comes from a valid source	Temporary blocking of emergency vehicle warning and other ITS messages from masqueraded emergency vehicle Accidents and general driver confusion if the source and contents of received messages cannot be relied upon General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages

Table 18: Consequences of threats to confidentiality in an ITS-S (Roadside)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Acquisition of personal information	- Eavesdropping	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver Some ITS BSA messages reveal the geographic location of the sending ITS-S	Without protection, any personal information exchanged in a unicast transaction could be intercepted and used by an attacker to gain illicit access to subscription services
Acquisition of behavioral details	- Eavesdropping - Traffic analysis	All ITS messages (even those associated with subscription services) are broadcast in the 5,9 GHz band and can, therefore, be intercepted by any capable receiver Some ITS BSA messages reveal the geographic location of the sending ITS-S	Analysis of message traffic can reveal which subscription services are being used by individual users. This information can be used to launch direct attacks on a particular ITS-S (Vehicle), such as an emergency vehicle. Analysis can also reveal behavioral information that can be used to launch a direct attack against an RSU (e.g. block the next RSU from services that use hand-over between RSUs)

Table 19: Consequences of threats to accountability in an ITS-S (Roadside)

Threat Group	Threat Type	Weakness	Undesirable Consequences
Denial of transmission	- Repudiation	There is no requirement for an RSU to maintain an auditable log of all or specific types of messages sent and received by it. Such a log should be maintainable for an RSU	Malicious and mischievous messages can be sent with impunity by a legitimate RSU as no proof exists that any particular message was ever sent by that particular RSU. Internal malware can be the cause of such behavior
Denial of data receipt	- Repudiation	There is no requirement for an RSU to maintain an auditable log of all or specific types of messages sent and received by it. Such a log should be maintainable for an RSU	Errors in service delivery cannot be traced back to the originating RSU. If the problematic RSU is not fixed, service errors may quickly affect a substantial amount of ITS-S (Vehicle)s

10.3 Security risks in an ITS system

10.3.0 Introduction

The method described in ETSI TS 102 165-1 [i.1] can be used to determine risk factors based upon the likelihood of a particular attack being successful and the impact that a successful attack would have on the system.

NOTE 1: The TVRA method specified in ETSI TS 102 165-1 [i.1] assigns the values of 1, 2 and 3 from the product of the derived threat impact and the likelihood of occurrence, to a risk level of "Minor" and only the value 4 to a risk of "Major". Use of the risk assessment algorithms in the ITS TVRA have shown that, in this particular application, a more even spread of values gives better results. Consequently, in this analysis the values 1 and 2 are assigned to a risk level of "Minor" while the values 3 and 4 are assigned to "Major".

NOTE 2: Risk estimations may change as a consequence of changes to the functional specifications. This means that the risk estimates in Table 18 and Table 19 are based on the functional descriptions that were available at the time of the estimation.

10.3.1 Risks in an ITS-S (Vehicle)

Table 20 identifies the risk of a successful attack on an ITS-S (Vehicle) in each threat group and various factors that are used in the formulation of that risk.

Table 20: Risk determination in an ITS-S (Vehicle)

Threat Group	Attack					Impact	Risk
	Factor	**Range**	**Value**	**Potential**	**Likelihood**		
DoS: Denial of access to incoming messages	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Specialized	3				
DoS: Denial of access to outgoing messages	Time	≤ 1 week	1	8 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Specialized	3				
DoS: Denial of access to internal resources	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				
Modification and deletion of stored information	Time	≤ 1 week	1	14 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				
Modification and deletion of transmitted information	Time	≤ 1 week	1	14 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				
Masquerade	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	2 (Medium)	4 (Major)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Standard	0				
Acquisition of personal information	Time	≤ 1 day	0	12 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Standard	0				
Acquisition of behavioral details	Time	≤ 1 day	0	18 (High)	1 (Possible)	2 (Medium)	2 (Major)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Difficult	12				
	Equipment	Specialized	3				
Acquisition of location information	Time	≤ 1 day	0	18 (High)	1 (Possible)	2 (Medium)	2 (Major)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Difficult	12				
	Equipment	Specialized	3				
Denial of transmission	Time	≤ 1 day	0	1 (No Rating)	3 (Likely)	1 (Low)	6 (Major)
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
Denial of data receipt	Time	≤ 1 day	0	1 (No Rating)	3 (Likely)	2 (Low)	6 (Major)
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				

10.3.2 Risks in an ITS-S (Roadside)

Table 21 identifies the risk of a successful attack on an ITS-S (Roadside) in each threat group and various factors that are used in the formulation of that risk.

Table 21: Risk determination in an ITS-S (Roadside)

Threat Group	Attack					Impact	Risk
	Attack	Range	Value	Potential	Likelihood		
DoS: Forgery of emergency vehicle warning	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Sensitive	4				
	Opportunity	Easy	1				
	Equipment	Standard	0				
DoS: Denial of access to incoming messages	Time	≤ 1 week	1	8 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Standard	0				
Modification and deletion of stored information	Time	≤ 1 week	1	14 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Proficient	2				
	Knowledge	Sensitive	4				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				
Masquerade as an emergency vehicle	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Standard	0				
Masquerade	Time	≤ 1 week	1	13 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Standard	0				
Acquisition of personal information	Time	≤ 1 day	0	7 (Basic)	3 (Likely)	3 (High)	9 (Critical)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Standard	0				
Acquisition of behavioral details	Time	≤ 1 day	0	18 (High)	1 (Possible)	2 (Medium)	2 (Major)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Difficult	1				
	Equipment	Specialized	0				
Denial of transmission	Time	≤ 1 day	0	1 (No Rating)	3 (Likely)	1 (Low)	3 (Major)
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
Denial of data receipt	Time	≤ 1 day	0	1 (No Rating)	3 (Likely)	1 (Low)	3 (Major)
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				

11 Countermeasures

11.1 List of Countermeasures

For each of the threats identified in the ITS TVRA it is necessary to consider what measures could be implemented to reduce the risk of an attack being successfully mounted on an ITS-S. Table 22 specifies a range of options to be evaluated as potential ITS countermeasures.

Table 22: Potential countermeasures to threats in an ITS system

Countermeasure	Threats	Risk
Reduce frequency of beaconing and other repeated messages	Message saturation	Critical
Add source identification (IP address equivalent) in V2V messages	Message saturation	Critical
Limit message traffic to V2I/I2V and implement station registration	Message saturation	Critical
	Injection of false messages	Major
	Manipulation of relayed ITS messages en route	Critical
	Masquerade as ITS-S (Vehicle or Roadside) or ITS network	Major
	Replay of "expired" (old) messages	Critical
	GNSS spoofing	Major
	Wormhole attacks	Major
	GNSS spoofing	Major
	Malicious isolation of one or more ITS-S (Vehicle) (black hole)	Critical
Implement frequency agility within the 5,9 GHz band	Jamming of radio signals	Critical
Implement ITS G5A as a CDMA/spread-spectrum system or base ITS on 3rd Generation mobile	Jamming of radio signals	Critical
Digitally sign each message using a Kerberos/PKI-like token system	Injection of false messages	Major
	Manipulation of relayed ITS messages en route	Critical
	Masquerade as ITS-S (Vehicle or Roadside) or ITS network	Major
	Replay of "expired" (old) messages	Critical
	Wormhole attacks	Major
	Malicious isolation of one or more ITS-S (Vehicle) (black hole)	Critical
Include a non-cryptographic checksum of the message in each message sent	Manipulation of relayed ITS messages en route	Critical
Remove requirements for message relay in the ITS BSA	Manipulation of relayed ITS messages en route	Critical
Include an authoritative identity in each message and authenticate it	Masquerade as ITS-S (Vehicle or Roadside) or ITS network	Major
Use broadcast time (Universal Coordinated Time - UTC - or GNSS) to timestamp all messages	Replay of "expired" (old) messages	Critical
	Wormhole attacks	Major
Include a sequence number in each new message	Replay of "expired" (old) messages	Critical
Use INS or existing dead-reckoning methods (with regular - but possibly infrequent - GNSS corrections) to provide positional data	Wormhole attacks	Major
	GNSS spoofing	Major
Implement differential monitoring on the GNSS system to identify unusual changes in position	Wormhole attacks	Major
	GNSS spoofing	Major
Encrypt the transmission of personal and private data	Eavesdropping	Critical
Implement a Privileged Management Infrastructure (PMI).	Installation of malware	Critical
Software quality and integrity are certified before it is installed	Installation of malware	Critical

Countermeasure	Threats	Risk
Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle	Traffic analysis	Minor
	Location tracking	Minor
Maintain an audit log of the type and content of each message sent from and received by an ITS-S	Denial of transmission	Critical
	Denial of data receipt	Critical
Include a source identity in each ITS message	Denial of transmission	Critical
Implement a non-repudiation framework	Denial of transmission	Critical
	Denial of data receipt	Critical
Plausibility checks on incoming messages	Injection of false messages	Major
	Manipulation of relayed ITS messages en route	Critical
	Masquerade as ITS-S (Vehicle or Roadside) or ITS network	Major
	Wormhole attacks	Major
Hardware-based protection of software and hardware configuration on ITS-S	Installation of malware	Critical
	Denial of transmission	Critical
	Denial of data receipt	Critical

11.2 Evaluation of Countermeasures

This evaluation of potential ITS security countermeasure makes the consequences of each countermeasure on the ITS architecture and the BSA explicit and identifies the security services needed to protect against the analysed security threats. The TVRA identified a number of problem areas in the ITS architecture, the communication protocols used for the ITS application in the BSA (CAM and DNM) and the underlying communication processes (e.g. beaconing and beaconing rate). The problem areas lead to a number of weaknesses in the ITS and these were also identified in the TVRA.

ETSI TS 102 165-1 [i.1] defines three levels of risk, *Minor*, *Major* and *Critical*, which are derived from a qualitative combination of likelihood and impact. The *Minor* risk level is the only one considered to be acceptable and, therefore, countermeasures should be introduced in order to reduce all *Major* or *Critical* risks to *Minor*.

There are two countermeasure strategies defined in the TVRA method, as follows:

i) asset redesign:

- removal of identified problem areas and weaknesses through fundamental design changes in the ITS standards specifying the architecture, protocols and communications processes;
- viability depends a number of factors which include the maturity of the affected ITS standards and the relative cost of removing the problem area as opposed to the simpler approach of masking it;
- can reduce both the likelihood and the overall impact of a successful attack.

ii) asset hardening:

- specification of additions to the ITS system that will mask the effects of a problem area rather than remove it completely;
- likely to be used in cases where:
  - the cost of asset redesign is unacceptable;
  - the change itself is unnecessarily complex; or
  - redesign does not reduce the risk level to *Minor*;
- can only affect the likelihood of a successful attack, not the impact.

11.3 Countermeasure Analysis

11.3.1 Reduce frequency of beaconing and other repeated messages

The use of beaconing (heartbeat) messages in V2V ITS and the repetition of some non-beacon messages generates considerable background radio traffic in high-density road-traffic environments. This countermeasure proposes to reduce the frequency of the beacon and other safety-of-life messages from 10 Hz to a lower number to reduce congestion. An alternative solution is to use adaptive frequency control where messages would be sent at different frequencies depending upon the nature of the message, the availability of 5,9 GHz bandwidth, and potentially other local conditions:

- Countermeasure strategy:
  - Asset redesign.
- Advantages:
  - Intrinsic saturation in ITS V2V is reduced.
- Disadvantages:
  - Safety-critical messages may not be received quickly enough by affected vehicles.
- Implications on ITS Architecture:
  - May affects the communication protocols for DNM and CAM.
- Implications on BSA:
  - Affects the communication frequency used to send ITS messages.
- Ability to remove relevant ITS problem areas:
  - Reduces the problem area of intrinsic high density of ITS messages traffic due to broadcasting and beaconing in V2V systems.

11.3.2 Add source identification (IP address equivalent) in V2V messages

A source address added to a V2V message should be identifiable by the ITS receiving station and non-forgeable so that the receiving station can trust that the source address has not been modified between the time of message origination and the time the message was received:

- Countermeasure strategy:
  - Asset hardening and redesign.
- Advantages:
  - Saturation messages can be identified and rejected within the ITS stack without the need to be processed by the associated application.
- Disadvantages:
  - The desired principles of anonymity within ITS are breached.
  - May not be available in the existing stack.
- Implications on ITS Architecture:
  - Changes to protocol stack for DNM and CAM.
- Implications on BSA:
  - None.

- Ability to remove relevant ITS problem areas:
    - Removes the problem of absence of addressing in broadcast messages meaning that the source of a message cannot be identified so malicious and irrelevant messages can only be rejected be the application, not on the network layer in the ITS stack.

11.3.3 Limit message traffic to V2I/I2V when infrastructure is available and implement message flow control and station registration

An ITS-S is required to register (and authenticate) to the ITS infrastructure either when it enters an administrative region or at each roadside unit that comes into range if the roadside infrastructure is not extensive. Once registered, the vehicle accepts and processes only messages received from the ITS infrastructure while it is in radio range. When no roadside unit is in range then the ITS-S will receive and process ITS messages from other vehicles:

- Countermeasure strategy:
    - Asset redesign:
        - The countermeasure will require redesign of the ITS architecture, the fundamental concept of V2V communications and the ITS protocols.
- Advantages:
    - RSU can issue "stop sending" command to saturating station.
    - The resources of the ITS network and information from other RSUs can be used to detect an attack and to formulate an integrated response to it (i.e. propagation and extent of warnings).
    - A registered offending station can be identified and removed from the system.
    - Messages can only be sent to and from registered, authenticated ITS stations.
    - The resources of the ITS network and information from other ITS stations can be used to detect an attack and to formulate an integrated response to it.
- Disadvantages:
    - It would be necessary to implement identity-based registration procedures between the vehicle and the ITS infrastructure.
    - The coverage of the ITS infrastructure would have to be extensive.
    - The speed of response to an incident would deteriorate (however, response times would be deterministic).
    - Registration requires a high density of roadside units at the borders between registration areas.
    - Current IEEE 802.11 [i.4] technologies do not support flow control.
- Implications on ITS Architecture:
    - May require separate frequency allocations for uplink and downlink.
    - Need to augment the architecture to support the ability to switch between V2I/I2V when available and purely V2V when infrastructure is not available.
    - The ITS system needs to ensure that a registration procedure should not disable an ITS-S (Vehicle) if it is interrupted by the vehicle passing out of range of the ITS-S (Roadside) to which it is registering.
- Implications on BSA:
    - Has implications on all V2V communication in the BSA.
- Ability to remove relevant ITS problem areas:
    - Removes the problem of lack of flow control in V2V broadcast messages.

  - Partly addresses the problem area of intrinsic high density of ITS messages traffic due to broadcasting and beaconing in V2V systems.
  - Partly addresses the absence of addressing in broadcast messages.

11.3.4 Implement frequency agility within the 5,9 GHz band

A radio transmission broadcast at the same frequency at all times can easily be overwhelmed by a higher-power signal at the same frequency. However, it is much more difficult to jam a transmission in which the radio frequency changes frequently within its defined band. If the changes in frequency and the intervals between changes are both determined on pseudo-random basis, it becomes even more difficult to jam the signal. There needs to be synchronization between the legitimate transmitter and the receiver and both need to use the same algorithms for determining frequency steps and the intervals between changes in frequency:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Jamming equipment need to be able to follow the shifts in frequency exactly. Without this facility they are unable to ensure continuous jamming.
- Disadvantages:
  - The ITS G5A frequency band is too narrow to support the number of frequencies required to make agility effective.
  - The cost of implementation is high as there is considerable added complexity in the radio subsystem.
  - As the algorithms for switching frequencies are embedded in each ITS-S, they will be publically available and, therefore, available for an attacker to acquire.
- Implications on ITS Architecture:
  - Additional hardware units would be required in an ITS-S to manage the frequency tuning of both the radio transmitter and the radio receiver.
  - No additional software entities would be required.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - The narrow band of frequencies available to the ITS radio system would make it difficult for an ITS-S to resist a sustained jamming attack for very long.

11.3.5 Implement ITS G5A as a CDMA/spread-spectrum system

Although considerably more complex than the narrowband radio proposed for ITS G5A, spread spectrum transmission of radio signals is naturally more resistant to both jamming and eavesdropping. As the Code Division Multiple Access (CDMA) schema used by spread spectrum transmission systems is based upon a pseudo-random sequence of codes, it is necessary for each ITS-S to have knowledge of this sequence:

- Countermeasure strategy:
  - Asset redesign:
    - ▪ The countermeasure will require a redesign of the appropriate ITS or IEEE standards.
- Advantages:
  - Spread spectrum radio transmissions automatically counter a narrowband jamming attack.

    - Spread spectrum transmissions are difficult to intercept for eavesdropping purposes.
    - CDMA would make duplex communication possible between a vehicle and the infrastructure and between vehicles.

- Disadvantages:
    - The cost of implementation is high as there is considerable added complexity in the radio subsystem.
    - CDMA cannot be used for V2V messaging.
- Implications on ITS Architecture:
    - Additional hardware units would be required in an ITS-S to manage the spreading of transmission frequencies and reception of spread signals.
    - No additional software entities would be required.
- Implications on BSA:
    - None.
- Ability to remove relevant ITS problem areas:
    - Spread spectrum transmission would remove the susceptibility to jamming of 5,9 GHz narrowband radio.

11.3.6 Integrate 3rd Generation mobile technology into ITS G5A communications

3rd Generation mobile communications (3G) already include comprehensive security functions and capabilities. A 3G connection to each vehicle will provide an alternative path for reporting a suspected 5,9 GHz jamming attack. It will also offer a secure route for any key and certificate management communications that may be required:

- Countermeasure strategy:
    - Asset redesign:
        - The countermeasure will require a redesign of the appropriate ITS standards.
- Advantages:
    - As a CDMA radio technology, 3G is automatically resilient to a narrowband jamming attack.
    - 3G transmissions are difficult to intercept for eavesdropping purposes.
    - 3G provides a secure communications path for reporting jamming attacks.
    - 3G provides a secure communications path for key and certificate management.
    - 3G provides fully duplex communications.
- Disadvantages:
    - Although the cost of implementation is not prohibitively high as the radio systems can be kept separate and 3G is a well established technology, the additional cost per user may not be acceptable.
- Implications on ITS Architecture:
    - Additional hardware units would be required in an ITS-S to handle 3G signalling but this would require only off-the-shelf items.
    - Software would need to distinguish between 5,9 GHz transmissions and 3G transmissions.
- Implications on BSA:
    - None.

- Ability to remove relevant ITS problem areas:
  - 3G would remove the susceptibility to jamming of some 5,9 GHz radio transmissions.
  - It will be possible for jamming attacks, once detected, to be reported to the ITS authority.

11.3.7 Digitally sign each message using a Kerberos/PKI-like token system

11.3.7.0 General

The recipient of a message can gain confidence in the message's origin, the permissions of the originator, and its integrity against changes in transit if the message includes a digital signature or other form of cryptographic checksum and the recipient has the means to check that the checksum is valid.

There are a two ways of cryptographically signing ITS messages:

- Symmetric (Kerberos-like):
  - Senders and receivers authenticate to a common server which issues both with sufficient credentials to establish the authority of the sender to transmit and the receiver to act upon messages exchanged subsequently between them.
  - Symmetric keys have a lifetime and are automatically invalidated when the lifetime expires and may be replaced.
- Public key (PKI-like):
  - Senders sign messages with a digital certificate issued by a Certification Authority (CA) and containing a public key. The recipient uses the public key from the certificate to verify the signature on the message. It also checks that the certificate is valid by, for example:
    - ensuring that it was issued by a known CA;
    - ensuring that it has not expired or been revoked; and
    - ensuring that the permissions it grants are consistent with the permissions the message sender is claiming in the certificate.

    These checks may be performed online or, if the receiver is not within radio range of an ITS-S (Roadside), using cached information.

    In the event that a known, valid ITS-S (Vehicle) is detected to be providing misleading information to other vehicles (either by malfunction or malicious intent), a CA may prevent other units from processing its messages by one or all of the following methods:

    - using a revocation process to distribute information about compromised units to ITS-S;
    - dynamically adjusting the frequency of distributing revocation information about compromised units; providing on-line status queries by message recipients;
    - issuing sender certificates with a limited lifetime, renewing them frequently and not reissuing certificates to devices that are known to be compromised.

11.3.7.1 Kerberos-like solution

11.3.7.1.1 General requirements

A secure implementation of a system based on Kerberos (IETF RFC 4120 [i.6]) depends on the availability of:

- keying material on the ITS-S to allow it to authenticate to the key server;
- access to the key server by a persistent communications mechanism;

- protection of the authentication keying material and other, transient keying material on an ITS-S; and
- access controls and software quality mechanisms to ensure that malicious software on the ITS-S cannot make use of the keys without extracting them.

11.3.7.1.2 Countermeasure analysis

- Countermeasure strategy:
    - Asset hardening.
- Advantages:
    - A unit that is discovered to be compromised can be prevented from accessing the system.
    - Symmetric key operations are very efficient and would not consume much processor power.
- Disadvantages:
    - Requires an always-on connection to avoid legitimate vehicles being locked out of the system. The management of keys and tokens greatly increases message traffic which may cause congestion if it is sent over 5,9 GHz but will require an additional communications medium if it is not sent over 5,9 GHz.
    - The system requires the infrastructure to detect a malfunctioning or malicious device and disable it. The device can continue to misbehave for the time that it takes identify it and prevent it from accessing the system.
    - Jurisdiction of key server may be complex.
- Implications on ITS Architecture:
    - There needs to be an always-on, always-available key server.
    - An ITS-S needs to be able to authenticate to a key server even when it is outside its country of origin.
- Implications on BSA:
    - Adds header information to BSA but does not affect the contents or use of BSA messages.
- Ability to remove relevant ITS problem areas:
    - Removes the problem of false message insertion.
    - Enables ITS-Ss that are sources for forged or otherwise inaccurate messages to be removed efficiently.
    - Does not on its own address acquisition of behavioral details or acquisition of personal information.

11.3.7.2 PKI-like solution

11.3.7.2.1 General requirements

A secure implementation of a system based on a Public Key Infrastructure (PKI) depends on the availability of:

- a secure provisioning system to allow an ITS-S to obtain certificates from the CA;
- timely; access to revocation information provided by the CA;
- dynamically adjusting the frequency of distributing revocation information about compromised units;
- protection of the authentication keying material and other, transient keying material on the ITS-S; and
- access controls and software quality mechanisms to ensure that malicious software on the ITS-S cannot make use of the keys without extracting them.

11.3.7.2.2 Countermeasure analysis

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - A unit that is discovered to be compromised can be disabled from the system.
  - The authorization system continues to operate even when there is no access to infrastructure.
- Disadvantages:
  - Public key operations are slow are slower symmetric key operations and may require specialized acceleration hardware.
  - Jurisdiction of CA may be complex.
  - With no access to infrastructure required, there may be a delay between the detection of a misbehaving ITS-S and its removal from the system.
  - The system requires the infrastructure to detect a malfunctioning device and disable it. The device can continue to misbehave for the time that it takes identify it and prevent it from accessing the system.
  - Distributing revocation information will cause congestion if it is sent over 5,9 GHz and will require an additional communications medium if it is not sent over 5,9 GHz.
- Implications on ITS Architecture:
  - There needs to be a CA that can distribute keys, certificates, and revocation information.
  - There needs to be a process for an ITS-S to receive an initial set of keys and certificates.
- Implications on BSA:
  - Adds header information to BSA but does not affect the contents or use of BSA messages.
- Ability to remove relevant ITS problem areas:
  - Removes the problem of false message insertion.
  - Enables ITS-Ss that are sources for forged or otherwise inaccurate messages to be removed efficiently.
  - Does not on its own address acquisition of behavioral details or acquisition of personal information.

11.3.8 Include a non-cryptographic checksum of the message in each message sent

A simple approach to protecting the contents of a transmitted ITS message is to include a checksum computed from the original contents. The receiving ITS-S is then able to calculate the checksum itself and compare it with the value included in the incoming message. If the checksum values do not match, the received message can be rejected. A simple longitudinal parity check would probably be insufficient for the purpose of establishing the integrity of a received ITS message but the more reliable Fletcher or Adler algorithms would provide the necessary protection. These algorithms, unfortunately, require more processing resources in both the sending and receiving ITS-S:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Accidental modification of the contents of a message en route can be detected.

- Disadvantages:
    - A subverted legitimate ITS-S possess all of the necessary algorithms to compute a valid checksum for a maliciously modified message.
- Implications on ITS Architecture:
    - Checksum creation and validation are provided as application layer security services.
- Implications on BSA:
    - None.
- Ability to remove relevant ITS problem areas:
    - Reduces the risk that messages will be accidentally modified en route.

11.3.9 Remove requirements for message relay in the ITS BSA

The propagation of ITS messages to emulate a wide-area broadcast (particularly in an emergency situation) is achieved by allowing an ITS-S (Vehicle) to re-broadcast any received message that has not reached the edge of its relevance area. Removing this capability makes it impossible for a message to be modified en route. This can only be achieved if the roadside infrastructure is sufficient to receive the original message and to transmit it across the whole of the relevance area:

- Countermeasure strategy:
    - Asset redesign.
- Advantages:
    - Messages are not re-transmitted so there is no opportunity for a message to be modified.
    - Message propagation does not depend on a particular density of vehicular traffic.
- Disadvantages:
    - Extensive roadside infrastructure would be necessary to ensure that messages reach the full extent of their relevance area.
- Implications on ITS Architecture:
    - None.
- Implications on BSA:
    - All messages which might have relevance outside the immediate radio coverage area of an ITS-S (Vehicle) would need to be sent V2I rather than V2V.
- Ability to remove relevant ITS problem areas:
    - Completely removes the possibility that a message could be modified en route between the originator and the receiver.

11.3.10 Include an authoritative identity in each message and authenticate it

An authoritative identity is produced and distributed by a commonly trusted entity in the ITS system. Such an identity is needed for an ITS station to verify the authenticity of the messages that it receives. This enables an ITS-S to verify that received messages come from valid and trustable sources. The authoritative identity is authenticated by the receiving station verifying the issuer of the authoritative identity. This means that the source itself is not authenticated but the fact that it was issued by a verifiable and commonly trusted authority:

- Countermeasure strategy:
    - Asset hardening.

- Advantages:
    - Authenticity of V2V ITS messages can be checked.
    - Authenticity of ITS messages can be verified in real-time and directly.

NOTE: There is a design decision that should be made and that is related to the trust period, meaning the frequency of updates of the common trusted authority and the credentials that this authority has issued and which are included in the message.

    - It becomes impossible for an attacker to masquerade as a legitimate ITS station.

- Disadvantages:
    - Authenticity of messages cannot be 100 % guaranteed as the authoritative identity is pre-issued which means that the source of an ITS message can be under attack even though the messages it sends includes a valid authoritative identity.
    - Requires regular updates and revocation of authoritative identity information.
    - It would be necessary to implement identity-based registration procedures between the vehicle and the ITS infrastructure.
    - The coverage of the ITS infrastructure would have to be extensive or it would be needed to accept a relative large time period that vehicles possibly can be under attack.
    - The speed of response to an incident would deteriorate.
- Implications on ITS Architecture:
    - Addition of authoritative entity and distribution and management of authoritative identities.
- Implications on BSA:
    - Addition of authority identity information to ITS messages (CAM and DNM).
- Ability to remove relevant ITS problem areas:
    - Including authoritative identity in ITS messages enables an ITS-S to check the authenticity of messages that it receives on lower levels in the protocol stack (network level).
    - The presence of an authoritative identity enables an ITS-S to check whether a received message comes from a source that the commonly trusted authority has approved and, from this information, it deduces that the information in the message is authentic and from an authentic source.
    - An ITS station can record information that later can be presented to an authority that knows the real identity of the authoritative identity included in the ITS message.

11.3.11 Use broadcast time (Universal Coordinated Time - UTC - or GNSS) to timestamp all messages

Including a timestamp in all messages makes it easier for a receiving ITS-S to judge whether a message is valid or not. If the time is derived from an external source such as Universal Coordinated Time (UTC) or GNSS ensures that each ITS-S uses the same time source as every other ITS-S. Consequently, it is quite simple for the plausibility of the timestamp in a message to be validated:

- Countermeasure strategy:
    - Asset redesign.
- Advantages:
    - Both UTC and GNSS can be used across all time zones without confusion and is broadcast on public FM radio channels (UTC) or satellite (GNSS).

  - ITS-S system time is derived from an independent source.
  - UTC and GNSS time spoofing attacks can be detected by differential monitoring.
- Disadvantages:
  - Neither broadcast UTC nor GNSS are well protected and may be easy to spoof.
  - Additional equipment is required in the ITS-S although this is likely to be either a GNSS receiver (which is required for other ITS capabilities) or a low-cost consumer radio controlled clock mechanism (which is available in many modern vehicles already).
- Implications on ITS Architecture:
  - None.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - The uncertainty about when a message was created is addressed. However, if the timestamp is not cryptographically bound to the message, the timestamp can be manipulated and replay is just as easy.

11.3.12 Include a sequence number in each new message

The validity of received messages can, in part, be established if each sender includes a sequence number in each message sent. Messages received out of sequence can be discarded as potentially false:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - It is possible to detect messages that are out of sequence.
- Disadvantages:
  - In an ITS system there is no guarantee that the integrity of a sequence will be maintained at the receiver, even in the absence of an attack.
  - It is difficult to coordinate sequence numbers between multiple sources of broadcast messages and associating sequences with specific sources may compromise privacy.
  - Sequence numbering does not prevent the replay of messages from a source that the receiver has never seen before.
  - Use of sequence numbers is impractical in V2V applications.
- Implications on ITS Architecture:
  - None.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - The uncertainty about when a message was created (in relation to previously messages received from the same source) is addressed. However, if the sequence number is not cryptographically bound to the message, it can be manipulated in a replay attack.

11.3.13 Use INS or existing dead-reckoning methods (with regular - but possibly infrequent - GNSS corrections) to provide positional data

GNSS is expected to be the only source of location information within ITS-S (Vehicle). As an external source of information it is possible for this to be mimicked such that the ITS-S is given incorrect data regarding its position. By using an onboard Inertial Navigation System (INS) or dead-reckoning derived from simple accelerometers such as those found in modern mobile phones it is possible for the ITS-S to determine its position from purely internal sources with only brief and infrequent references to GNSS for waypoint corrections:

- Countermeasure strategy:
  - Asset redesign.
- Advantages:
  - An ITS-S (Vehicle) can have greater confidence in its location so that it can resist, in particular, wormhole attacks.
  - Current position coordinates can be determined in the absence of a GNSS signal.
  - From an initial location fix, INS can provide a very accurate and ongoing determination of the vehicle's position over a long period.
  - Accelerometers for dead-reckoning add little to the cost of the ITS-S.
- Disadvantages:
  - INS equipment adds a considerable amount to the cost of the ITS-S.
  - Dead-reckoning requires considerable processing resources.
  - Dead-reckoning is not as accurate as either GNSS or INS.
  - Both INS and dead-reckoning require access to GNSS for mid-course corrections.
- Implications on ITS Architecture:
  - INS is installed as a data source external to the ITS-S.
  - Dead-reckoning may require a processing entity to calculate current location from accelerometer inputs.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - Significantly removes the possibility of GNSS spoofing attacks. Even in the presence of a such an attack, the ITS-S would be able to determine whether its mid-course GNSS corrections were plausible or not.

11.3.14 Implement differential monitoring on the GNSS system to identify unusual changes in position

A GNSS system determines the position of a vehicle by reference to three different GNSS satellites.

Differential GNSS is a way of correcting various inaccuracies in a GNSS system and, thus, providing more accurate position information. It involves the cooperation of one normal receiver and a reference receiver which is used to measure timing errors. From this it is able to provide correction information to the normal receiver. The reference receiver is placed and maintained in a known location so that its position is always known. It receives the same GNSS signals as the roving receiver but instead of working like a normal GNSS receiver it analyses the received data by applying the position solving equations backwards. Instead of using timing signals to calculate its position, it uses its known position to calculate timing. From this information it deduces what the travel time of the GNSS signals should be and compares it with what they actually are. The difference is called an error correction factor.

The benefit of differential GNSS is that it is capable of positioning things very precisely and this feature can be used to detect even small abnormalities in position errors. A successful GNSS spoofing attack can then only alter a vehicle's true position within the acceptable error space. Differential GNSS monitoring can also detect very small and marginal abnormal changes within the normal error space. The principles of differential GNSS can be implemented in an ITS-S as a software solution which can detect errors in GNSS location information in real-time for both vehicles and RSUs. This solution requires reference points with know locations that communicate with the differential monitoring module in a vehicle. For example, all RSUs have a know location and can aid vehicles in real-time in cases where a vehicle has contact with one or more RSUs:

- Countermeasure strategy:
  - Asset redesign.
- Advantages:
  - Improves accuracy of on-board GNSS data.
  - Does not involve large costs (less costly than INS).
  - Easily implemented in simple software.
- Disadvantages:
  - Not as accurate as INS and may not be sufficient to detect all attacks.
  - May need to use RSU or other stationary ITS units as the reference receiver to maximize the accuracy.
- Implications on ITS Architecture:
  - Addition of differential monitoring module for the GNSS system in vehicles.
  - Addition of reference receiver capabilities.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - The reference receiver can be used to aid vehicles in checking validity of messages and to synchronize the source of timestamp creation.

11.3.15 Encrypt the transmission of personal and private data

Personal and private data covers all pieces of information in ITS messages that can be used to positively identify a vehicle, an ITS user, the location and behavior of a particular vehicle or its route. By encrypting personal and private data it is possible to ensure that traffic analysis and eavesdropping alone cannot reveal sufficient information to directly extract or indirectly deduce private information:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Personal and private information is not sent in clear text over the air.
  - Behavior of particular vehicles cannot easily be deduced.
  - Transmitted data can only be understood by a receiving station equipped with the necessary keys (it has to know the key used to encrypt the personal data) and decryption facilities.
- Disadvantages:
  - Encryption is a realistic option only on non-broadcast transmissions.

    - The implementation of encryption capabilities is both expensive and resource-consuming.
    - Cryptographic separation needs to be applied at the higher layers of the protocol stack.
- Implications on ITS Architecture:
    - May affect the size of ITS messages depending on whether compression is combined with encryption.
    - Adds key distribution and management services to the ITS architecture.
    - Adds encryption capabilities to ITS stations.
    - Introduces delay upon reception and sending of messages with personal content.
- Implications on BSA:
    - No direct implications.
- Ability to remove relevant ITS problem areas:
    - Encryption of data within an ITS message is only effective as a countermeasure on messages that are directed to a specific location (i.e. V2I or I2V). Its effect on broadcast messages is negligible as all ITS stations possess the keys required to decrypt encrypted messages.

11.3.16 Implement a Privilege Management Infrastructure (PMI)

A Privilege Management Infrastructure (PMI) is a cryptographic certificate-based approach to asserting the rights of a user or application to access or modify data or executables within a system. Examples of PMIs are Recommendation ITU-T X.509 [i.5] or the Security Assertion Markup Language (SAML).

Any attempt to modify ITS-S configuration information or to insert new or revised software needs to be accompanied by a certificate that establishes the user's right to make such a change.

A PMI carries user privileges in the form of attributes in an Attribute Certificate (AC). A Source of Authority (SoA) and an Attribute Authority (AA) issue Acs to users in much the same way that a Certification Authorities (CA) issues PKCs to users. PMIs usually rely on an underlying PKI as Acs need to be digitally signed by the issuing AA and the PKI is used to validate the AA's signature:

- Countermeasure strategy:
    - Asset redesign and asset hardening.
- Advantages:
    - Configuration changes can only be made by authorized users or applications.
    - Software updates and extensions can only be installed by authorized users or applications.
- Disadvantages:
    - PMI adds a further level of key management to an ITS system.
    - All of the same issues related to certificate maintenance and revocation that have been identified for PKI (clause 11.3.7.2) also exist in PMI.
- Implications on ITS Architecture:
    - PMI is implemented as an application layer security service.
- Implications on BSA:
    - None.
- Ability to remove relevant ITS problem areas:
    - PMI protects an ITS-S against the installation of malware.

- PMI protects an ITS-S against malicious modification of its configuration data.

11.3.17 Software authenticity and integrity are certified before it is installed

By certifying the authenticity and integrity of ITS-S software it is possible to ensure that only authorized updates and extensions can be downloaded to the ITS-S. Mechanisms for restricting the applications that can be installed on a system ITS-S should be in place. An example of such a mechanism is the Java Code Signing which only permits software that has been digitally signed by a trusted third party to run within its virtual machine to. In general, a signature is included over the application package together with a certificate of the signing trusted third party:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Only software known to the ITS operator is installed on an ITS-S.
  - Certification of software integrity prevents the installation of malware on an ITS-S.
- Disadvantages:
  - Certification process and infrastructure can be extensive and complex to implement for suppliers.
- Implications on ITS Architecture:
  - Certificate management infrastructure is necessary.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - Restricting which applications can run on a particular platform covers many threats related to denial of service and the modification and deletion of stored information.
  - The level of protection depends on the rules in place to check software authenticity and restrict access to the ITS station. Hardware based security is significantly better than a pure software based solution but also more expensive.

11.3.18 Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle

Messages originating from an ITS-S may contain different identifiers at each layer of the ITS protocol stack. Particularly at the application layer, such identifiers may carry information that can identify the user or vehicle. Examples of this information include driver's name, driver's address, vehicle license plate or VIN. To prevent an eavesdropper from acquiring this personal information, an ITS-S can use identifiers, generally referred to as "pseudonyms", that are not directly linked to the user's true identity. The use of pseudonyms can only be considered effective if the method used is able to guarantee that:

- the user's true identity is hidden from all other users;
- the user's true identity cannot be derived from observation of that user's behavior (use of ITS services).

This does not prevent an attacker from visually identifying a vehicle and getting its license plate number (or recognizing the driver). However, the use of pseudonyms ensures that linking involves some activity outside the 5,9 GHz band:

- Countermeasure strategy:
  - Asset redesign.

- Advantages:
  - An eavesdropper's cannot identify a vehicle's owner without making an observation outside the 5,9 GHz band.
- Disadvantages:
  - Pseudonyms make it more difficult to identify and remove a misbehaving ITS-S. It is, therefore, necessary for an ITS authority to be able to resolve a pseudonym back to a true identity.
  - Managing pseudonyms, especially those issued by a Trusted Third Party (TTP), is complex and expensive when compared with existing non-pseudonym based solutions.
- Implications on ITS Architecture:
  - An ITS-S requires a means of obtaining or deriving a pseudonym.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - The use of pseudonyms means that users cannot be directly identified by analysis of received ITS messages.
  - It is difficult to associate the use of specific ITS services with specific users.

11.3.19 Maintain an audit log of the type and content of each message sent to and from an ITS-S

An ITS-S records in memory details of all messages sent and received by the ITS-S. Although this cannot be considered to be a definitive record, it can provide useful information in the event of a dispute or a road traffic incident. The contents of the audit log cannot be modified or deleted retrospectively by the ITS-S (Vehicle) operator; it is only available to ITS and law enforcement authorities:

- Countermeasure strategy:
  - Asset redesign.
- Advantages:
  - The audit log records the receipt of all incoming messages.
  - The audit log records the transmission of all outgoing messages.
- Disadvantages:
  - The integrity of the audit log requires protection.
  - Sufficient additional memory is required within an ITS-S to maintain an audit log for the duration of the period between servicing of the vehicle.
- Implications on ITS Architecture:
  - Increases storage space requirements for ITS station units.
  - Add audit log protection and maintenance.
- Implications on BSA:
  - None.

- Ability to remove relevant ITS problem areas:
  - The presence of an audit log limits the ability of a vehicle operator to repudiate the transmission or receipt of specific ITS messages in the event of a dispute.

11.3.20 Perform plausibility tests on incoming messages

Plausibility checks are non-cryptographic measures which use rules and other mechanisms to determine the likelihood that received data is correct. These rules and mechanisms range from simple heuristics to quite sophisticated and more complex, methods.

An ITS-S receives messages at regular and frequent intervals from ITS-equipped vehicles which are within radio range of it. These messages contain information regarding the senders position and status and, potentially, the time at which the message was sent. By correlating this information with data previously received from the same source as well as data received from other vehicles, it is possible for the receiving ITS-S to detect any anomalies (for example, implausible shifts in time or position) and reduce the level of trust it associates with the sending ITS-S:

- Countermeasure strategy:
  - Asset redesign and asset hardening.
- Advantages:
  - No cost for infrastructure, little cost for integration.
  - Low resource requirements.
  - May provide sufficient assurance that data is correct - depending on the application.
  - May need to be part of many applications (as relevance check) anyway.
  - Detects malicious attacks as well as malfunctioning ITS-Ss.
- Disadvantages:
  - Will not detect sophisticated attacks where time, position and status data are modified gradually over a longer period of time.
- Implications on ITS Architecture:
  - Validation of plausibility is provided as security services at the application and lower layers of the ITS stack.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - Restricts the values an attacker could use to inject a false message or manipulate a message en route.
  - Does not remove the threat of masquerading except where the attacker assumes properties the faked unit could not possibly have (such as a moving RSU).
  - Reduces the risk of wormhole attacks.

11.3.21 Provide remote deactivation of misbehaving ITS-S (Vehicle)

By collecting and collating information provided by ITS-S (Vehicle)s and other sources, the ITS infrastructure deduces that a particular ITS-S (Vehicle) is misbehaving either maliciously or through a system failure. To avoid continuing disruption to other vehicles, the infrastructure is able to remotely deactivate transmissions from the misbehaving ITS-S (Vehicle) while leaving able to receive transmissions from other stations:

- Countermeasure strategy:
  - Asset redesign.
- Advantages:
  - An ITS-S (Vehicle) can be remotely shut down if it is causing problems to other ITS users.
  - In times of heavy vehicular and communications traffic, a proportion of the broadcasting ITS stations can be temporarily prevented from sending messages (a basic form of flow control).
- Disadvantages:
  - The detection of a misbehaving ITS-S (Vehicle) requires cooperation between the infrastructure and other vehicles and may not be timely or definitive.
  - It will not be possible to deactivate special equipment designed specifically for an attack on the ITS system.
- Implications of ITS Architecture:
  - Adds the requirement for the control of transmission hardware in the ITS-S.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - Makes it possible for the ITS infrastructure to disable an ITS-S once it has detected that it is misbehaving.
  - Provides a measure of flow control which can be used to reduce excessive message densities in times of overload.

11.3.22 Use hardware-based identity and protection of software on an ITS-S

Hardware-based protection allows for secure storage and maintenance of software, OS and platform configuration of ITS-S. This is of particular importance for software updates to ITS applications in the BSA or security parameter updates over the air (and not on location at the vehicle manufacturer). In this context, hardware-based encryption seeds (keying generation information and keys) are stored locally and not sent over the air link and are therefore never exposed to outsiders. Immutable persistent units are not changeable after card production and represent the strongest possible storage of encryption seeding information. Hardware-based identity can be used to derive temporary identities that can be used for communication without revealing the real identity of an ITS station. This identity can also be used as a basis for pseudonym generation and to derive addressing information suitable for checking the authenticity of a message originator:

- Countermeasure strategy:
  - Asset redesign.
- Advantages:
  - Hardware-based protection parameters cannot easily be accessed and changed (if stored in immutable persistent unit, such information can never be changed after production of the hardware chip).
  - Hardware-based protection parameters are never transmitted over the air.

  - Hardware-based identity (preferably an immutable persistence stored identity) can be used in an IAAA schema.
  - Hardware-based identity adds addressing capabilities that can be used in DNM and CAM messages without revealing the true identity of an ITS station.

- Disadvantages:
  - An additional hardware chip containing identity and encryption information is required.
  - An additional trust relationship needs to be maintained between the card issuer and the vehicle manufacturer.

- Implications on ITS Architecture:
  - Changes lower layers of the ITS architecture.
  - Adds hardware-based identification and addressing information to CAM and DNM messages.

- Implications on BSA:
  - None.

- Ability to remove relevant ITS problem areas:
  - The true identity of an ITS station stored in an immutable persistent unit can easily be protected and used to derive temporary identity and addressing information. This can then be added to CAM and DNM messages without exposing the true identity of a vehicle or any private and sensitive information on the whereabouts, behavior or characteristics of a vehicle.
  - An ITS-S (Roadside) can resolve the hardware-based temporary identity of an offending ITS-S (Vehicle) to its true identity by reference to an authoritative entity within the ITS infrastructure.
  - Hardware-based identity can be used as the basis of the identification, authentication and authorization schema in ITS in addition to hardware-based protection of software, OS and platform configuration information.
  - Address information can be added to broadcast messages so that the originator can be identified without revealing the its true identity. Malicious and irrelevant messages can then be rejected at the network layer in the ITS stack rather than within applications.

11.4 Countermeasure Set

11.4.0 Introduction

Countermeasures can have two purposes in a system. They can remove one or more of the identified ITS problem areas or the can protect against one or more of the identified threats. Some countermeasures address both purposes.

The problem areas identified in ITS (Table 8 and Table 14) are:

- Intrinsic high density of ITS message traffic due to broadcasting and beaconing in V2V systems.
- Lack of flow control in V2V broadcast messaging.
- Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected by the application, not at the network layer in the ITS stack.
- The sub-optimal use of the available bandwidth caused by the random re-attempt period in the "Listen before send" message transmission method.
- Inability of the ITS-S (Vehicle) to quickly detect and isolate interference on radio channels.
- CAM and DNM messages do not include any form of identification information.

- Vehicle-to-Vehicle messages include no validation or legitimacy checks.
- Uncertainty regarding how timestamps are created and how to use them to check the validity of messages.
- ITS-S (Vehicle) memory can be modified by information received over the air interface.
- Broadcast messages are in general intended for all ITS-S within range.

The threats identified in ITS are:

- Denial of service and availability threats:
  - message saturation;
  - jamming of radio signals;
  - injection of false messages;
  - wormhole attacks.
- Integrity and masquerade threats:
  - manipulation of relayed its messages en route;
  - masquerade as its station or its network;
  - replayed of "expired" (old) messages;
  - GNSS spoofing;
  - malicious isolation of one or more ITS-S (Vehicle) (black hole);
  - installation of malware.
- Confidentiality and privacy threats:
    - eavesdropping;
    - traffic analysis;
    - location tracking.
- Accountability and non-repudiation threats:
  - denial of transmission;
  - denial of data receipt.

11.4.1 ITS Countermeasure Set

11.4.1.1 Countermeasures to Denial of Service (DoS) and availability threats

The following countermeasures address threats to DoS and availability:

1) Limit message traffic to V2I/I2V when infrastructure is available and implement message flow control and station registration:
   - removes the problem of lack of flow control in V2V broadcast messages;
   - removes the problem that broadcast messages are intended for all ITS-Ss within range;
   - addresses the absence of addressing in broadcast messages. Without any address, the source of a message cannot be identified so malicious and irrelevant messages can only be rejected by the application, not at the network layer in the ITS stack;
   - addresses the problem that broadcast messages are in general intended for all ITS-Ss within range;

- partly addresses the "Listen before send" problem in the message transmission method;
- Provides protection against masquerade, wormhole attacks and message saturation to some extent.

2) Include a sequence number in each new message:

   - removes the problem area of lack of flow control in V2V broadcast messages when implemented together with the V2I/I2V countermeasure;
   - when used together with V2I/I2V this countermeasure provides protection against the replay of "expired" old messages and therefore provides protection against the "Injection of false messages" and "Manipulation of relayed ITS messages en route".

3) Reduce the frequency of beacon and other repeated messages when flow control is not available:

   - removes the problem of the intrinsic high density of ITS messages traffic due to broadcasting and beaconing in V2V systems;
   - reduces the problem of limited bandwidth associated with the "Listen before send" message transmission method;
   - provides protection against message saturation.

4) Add source identification across the stack in ITS messages:

   - removes the problem of lack of flow control in V2V broadcast messages;
   - removes the problem of absence of addressing in broadcast messages. Without any address, the source of a message cannot be identified so malicious and irrelevant messages can only be rejected by the application, not at the network layer in the ITS stack;
   - removes the problem that CAM and DNM messages do not include any form of identification information.

5) Provide remote deactivation of misbehaving devices capability (includes capability of detecting misbehaving devices):

NOTE: This countermeasure assumes the existence of functions capable of detecting misbehaving devices and should be used together with an alternative communication path to remove misbehaving devices.

   - protects against:
     - malicious isolation of one or more ITS-S (Vehicle);
     - message saturation;
     - injection of false messages;
     - replay of old messages; and
     - wormhole attacks.

6) Alternative communication path to remove misbehaving devices and to download security management information:

   - works together with remote deactivation of misbehaving devices to protect against:
     - installation of malware;
     - manipulation of relayed ITS messages en route;
     - DoS attacks (partially); and
     - manipulation attacks (partially).

7) Implement frequency agility within the G5A:

   - removes the problem of the inability of an ITS-S (Vehicle) to quickly detect and isolate interference on radio channels;

   - provides protection against jamming of radio signals.

11.4.1.2 Countermeasures to integrity threats

The following countermeasures address threats to integrity:

1) Include a non-cryptographic checksum of the message in each message sent with forward error correction:

   - addresses the problem that Vehicle-to-Vehicle messages include no checks on the integrity or legitimacy of the content of the message;

   - provides protection against manipulation of relayed ITS messages en route and replay of "expired" old messages.

2) Include an authoritative identity in each message and authenticate it:

   - enables the receiver to check the source and authenticity of a message thus removing the problem that Vehicle-to-Vehicle messages include no integrity or legitimacy checks;

   - provides protection against manipulation of relayed ITS messages en route and replay of "expired" old messages.

3) Implement plausibility validation on incoming messages:

   - removes the problem that Vehicle-to-Vehicle messages include no integrity or legitimacy checks;

   - provides protection against GNSS spoofing and manipulation of relayed ITS messages en route.

4) Use broadcast time (Universal Coordinated Time (UTC) or GNSS) to timestamp all messages:

   - removes the problem of uncertainty regarding how timestamps are created and how to use them to check the validity of messages;

   - provides protection against GNSS spoofing and replay of "expired" old messages.

5) Hardware-based protection of software and hardware configuration on ITS-S:

   - provides protection against installation of malware.

6) Software authenticity and integrity are certified before it is installed:

   - removes the problem that ITS-S (Vehicle) memory can be modified by information received over the air interface;

   - provides protection against installation of malware.

11.4.1.3 Countermeasures to confidentiality and privacy threats

The following countermeasures address threats to confidentiality and privacy:

1) Digitally sign each message using a Kerberos/PKI-like token system:

   - addresses the problem that CAM and DNM messages do not include any form of identification information;

   - addresses the problem that Vehicle-to-Vehicle messages include no integrity or legitimacy checks;

   - provides protection against masquerade and spoofing attacks depending on its implementation and the management of security information (security information should be distributed over the alternative communication path).

2) To identify the sender or receiver of a message, use a pseudonym that cannot be linked to either the user's true identity or the identity of the user's vehicle:

   - provides protection against traffic analysis and location tracking.

3) Encrypt the transmission of personal and private data:

   - provides protection against:
     - eavesdropping;
     - traffic analysis;
     - acquisition of behavioral details;
     - acquisition of personal information; and
     - location tracking.

11.4.1.4 Countermeasures to non-repudiation and accountability threats

The following countermeasures address threats to non-repudiation and accountability:

1) Add an audit log to ITS stations to store the type and content of each message sent to and from an ITS-S:

   - the presence of an audit log limits the ability of a vehicle operator to repudiate the transmission or receipt of specific ITS messages in the event of a dispute;
   - provides protection against denial of transmission and data receipt.

2) Include source identity in each ITS message:

   - enables the receiver to check the source of a message and therefore removes part of the problem that Vehicle-to-Vehicle messages include no integrity or legitimacy checks;
   - provides protection against denial of transmission and data receipt when used together with the audit log countermeasure.

11.4.2 Residual risk

The countermeasure set described in clause 11.4.1 removes all of the problem areas identified in Table 8 and Table 14 and provides protection against all identified threats. However, countermeasures against misbehaving units depend on those units being identified immediately and the nature of the ITS system makes this almost impossible to achieve. With this exception, there are no residual risks provided that the countermeasure set are deployed according to ETSI TS 102 731 [i.2].

NOTE: As all identified threats can be countered with the measures described in clause 11.4.1, any countermeasures described in clause 11.3 but not included in the countermeasures set are not considered further in the present document or in ETSI TS 102 731 [i.2].

Annex A:
Cost - Benefit analysis of the selected countermeasures

As a guide to the value of implementing each of the countermeasures described in clause 11.3, a simple Cost-Benefit analysis was performed on each of them. The analysis took the following factors into consideration:

- Costs:
  - the extent to which the ITS standards would require modification and extension;
  - the extent to which the implementation of the countermeasure would require additional engineering development and special test equipment;
  - the extent to which the ongoing costs of manufacture of the ITS-S and the costs of managing and maintaining the ITS infrastructure would be extended by the existence of the countermeasure;
  - an estimation of any negative impact that the countermeasure would have on the ITS system's ability to comply with regulatory requirements;
  - an estimation of any negative impact that the countermeasure would have on market acceptance of ITS as a whole.
- Benefits:
  - the extent to which implementation of the countermeasure reduces the evaluated risk level associated with each threat group affected by the countermeasure;
  - an estimation of any positive impact that the countermeasure would have on the ITS system's ability to comply with regulatory requirements;
  - an estimation of any positive impact that the countermeasure would have on market acceptance of ITS as a whole.

The results of the Cost-Benefit analysis, as it applies to the countermeasures included in the countermeasure set described in clause 11.4.1, is shown in Table A.1.

Table A.1: Summary of Cost-Benefit analysis on the selected ITS countermeasures

Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Reduce frequency of repeated messages	**Standards design**	Low Impact	**Minor**	0	0	**9**
	Implementation	No Impact	**Major**	0	2	
	Operation	No Impact	**Critical**	3	1	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		
Include source address in all V2V messages	**Standards design**	Medium Impact	**Minor**	0	1	**14**
	Implementation	Medium Impact	**Major**	1	3	
	Operation	No Impact	**Critical**	3	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			No Impact		
Limit message traffic to V2I/I2V	**Standards design**	Major Impact	**Minor**	0	5	**17**
	Implementation	Major Impact	**Major**	2	1	
	Operation	Major Impact	**Critical**	4	0	
	Regulatory Impact			Significant Positive Impact		
	Market Acceptance			No Impact		
Implement frequency agility within the 5,9 GHz band	**Standards design**	Major Impact	**Minor**	0	0	**-21**
	Implementation	Major Impact	**Major**	0	2	
	Operation	Medium Impact	**Critical**	2	0	
	Regulatory Impact			Severe Negative Impact		
	Market Acceptance			No Impact		
Alternative communications path for security management purposes	**Standards design**	Medium Impact	**Minor**	0	3	**19**
	Implementation	Medium Impact	**Major**	0	0	
	Operation	Low Impact	**Critical**	3	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			No Impact		
Implement plausibility validation on incoming information	**Standards design**	Medium Impact	**Minor**	0	3	**25**
	Implementation	Medium Impact	**Major**	1	2	
	Operation	No Impact	**Critical**	4	0	
	Regulatory Impact			No Impact		
	Market Acceptance			Positive Impact		
Include a non cryptographic checksum of the message in each message sent	**Standards design**	Low Impact	**Minor**	0	0	**3**
	Implementation	Low Impact	**Major**	0	1	
	Operation	No Impact	**Critical**	1	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		
Use broadcast time (Universal Coordinated Time - UTC - or GNSS) to timestamp all messages	**Standards design**	Low Impact	**Minor**	0	2	**6**
	Implementation	Medium Impact	**Major**	1	1	
	Operation	Low Impact	**Critical**	2	0	
	Regulatory Impact			Negative Impact		
	Market Acceptance			No Impact		

Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Include a sequence number in each new message	**Standards design**	Low Impact	**Minor**	0	0	**7**
	Implementation	Low Impact	**Major**	1	3	
	Operation	Low Impact	**Critical**	2	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		
Software authenticity and integrity are certified before it is installed	**Standards design**	Medium Impact	**Minor**	0	4	**23**
	Implementation	Major Impact	**Major**	0	0	
	Operation	Medium Impact	**Critical**	4	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			Positive Impact		
Include an authoritative identity in each message and authenticate it	**Standards design**	Medium Impact	**Minor**	0	2	**11**
	Implementation	Major Impact	**Major**	1	2	
	Operation	Low Impact	**Critical**	3	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			No Impact		
Encrypt the transmission of personal and private data	**Standards design**	Major Impact	**Minor**	0	0	**-1**
	Implementation	Major Impact	**Major**	0	1	
	Operation	Low Impact	**Critical**	1	0	
	Regulatory Impact			Significant Positive Impact		
	Market Acceptance			Positive Impact		
Use hardware-based identity and protection of software on an ITS-S	**Standards design**	Low Impact	**Minor**	0	2	**12**
	Implementation	Medium Impact	**Major**	0	1	
	Operation	Medium Impact	**Critical**	3	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		
Add an audit log to ITS stations to store the type and content of each message sent to and from an ITS-S	**Standards design**	Low Impact	**Minor**	0	2	**8**
	Implementation	Low Impact	**Major**	2	0	
	Operation	Low Impact	**Critical**	0	0	
	Regulatory Impact			Significant Positive Impact		
	Market Acceptance			Negative Impact		
Digitally sign each message using a Kerberos/PKI-like token	**Standards design**	Medium Impact	**Minor**	0	1	**9**
	Implementation	Major Impact	**Major**	1	4	
	Operation	Major Impact	**Critical**	4	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			Positive Impact		
Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle	**Standards design**	Medium Impact	**Minor**	0	2	**5**
	Implementation	No Impact	**Major**	2	0	
	Operation	Low Impact	**Critical**	0	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			No Impact		

Countermeasure	Cost		Benefit			Result
	Category	**Value**	**Risk Level**	**Original Count**	**Revised Count**	
Allow remote activation and deactivation of ITS-S	**Standards design**	Medium Impact	**Minor**	0	4	**9**
	Implementation	Major Impact	**Major**	1	0	
	Operation	Major Impact	**Critical**	3	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			No Impact		

Annex B: GeoNetworking Risk Assessment

B.1 Introduction

In the following, a risk assessment of GeoNetworking is performed. GeoNetworking is specified in ETSI TS 102 636-4-1 [i.7]. Note that only ETSI EN 302 636-4-1 [i.10] (media independent functionality) is analysed here.

NOTE: It is assumed that all ITS-S GeoAdhoc routers implement the same minimum security measures and especially apply cryptographical protection (packets signature) as defined in ETSI EN 302 636-4-1 [i.10], clause 7.

B.2 GeoNetworking Model

GeoNetworking provides self-organized communication among ITS-Ss and makes use of geographical positions for packet transport over short-range wireless technology, such as ITS-G5. GeoNetworking supports the communication among individual ITS stations as well as the distribution of packets in geographical areas.

GeoNetworking defines three roles of an GeoAdhoc router, i.e. source, sender, forwarder, receiver and destination (see ETSI EN 302 636-4-1 [i.10] for the definition. GeoNetworking supports the following packet transport types:

1) GeoUnicast (GUC): Communication from a source to a destination.

2) Topologically-Scoped Broadcast (TSB): Communication from a source to all nodes in n-hop communication range.

3) Single-Hop Broadcast (SHB): Communication from a source to all nodes in single hop communication range, i.e. to the neighbor nodes.

4) GeoBroadcast (GBC): Communication from a source to all nodes inside a geographical target area.

5) GeoAnycast (GAC): Communication from a source to any node inside a geographical target area.

For GBC and GAC, the source does not need to be inside the geographical target area. In this case, the packet is transported towards the destination area, potentially via multi-hop communication.

An ITS-S can act as vehicle ITS-S and road-side ITS-S and each ITS-S instantiation can potentially communicate with each other. All communication models can be used in a vehicle-to-vehicle or vehicle-to-infrastructure (road-side ITS-S) manner. A foreseen connectivity scenario is displayed below in Table B.1.

B.3 Packet Structure

A GeoNetworking packet consists of payload, common header, and extended header. These are defined in Table B.1.

Table B.1: GeoNetworking Packet Structure

Basic Header	Basic information about the packet	The Basic Header is used to specify the version of the GeoNetworking protocol, the type of header immediately following the GeoNetworking Basic Header, the maximum tolerable time a packet can be buffered until it reaches its destination and remaining hop limit.
Common Header	Information about the packet	The Common Header is used to specify the information of the packet, e.g. type of the next header (Extended Header). It is also generated by the originator and not modified by intermediate sender ITS-S.
Extended Header	(Originator) Source address (Originator) Source location Target address/target location	The Extended Header is generated by the originator ITS-S. It is typically not modified by intermediate sender ITS-S. The target address might be updated by an intermediate ITS-S though. The source address and location might be used by receivers to update the location table.
Payload	Packet payload	E.g. CAM or DENM message packets.

B.4 Target of Evaluation

B.4.1 General

The Target of Evaluation (ToE) is displayed in Figure B.1.

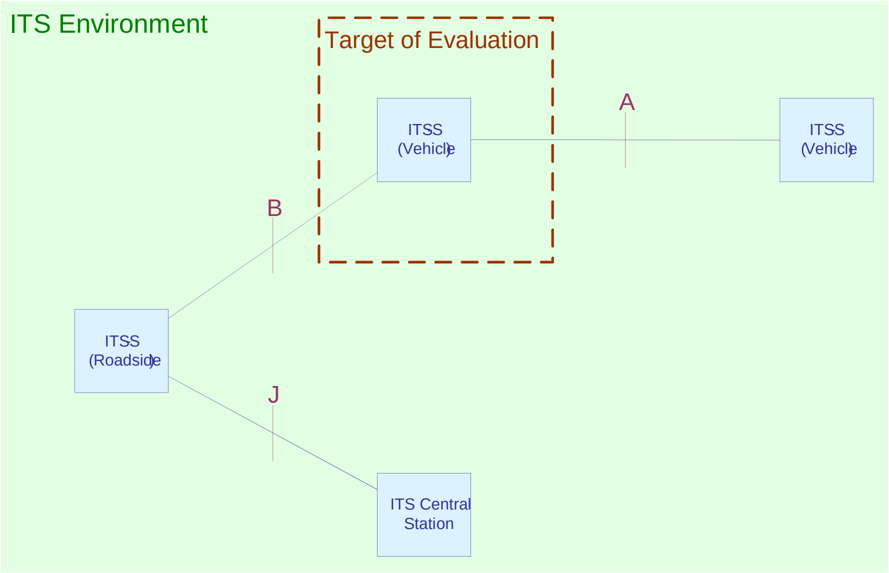

Figure B.1: ITS-S (Vehicle) as ToE

B.4.2 Assumptions

The assumptions of clauses 8.1 and 8.2 are used. However, they are extended by the assumption that ITS-S will communicate via 5,9 GHz channel.

B.4.3 Assets

B.4.3.1 Data Assets

Data assets of the payload include the case described in clause 9.

Data also includes information used for routing, such as speed, heading, location, and accuracy. This information is sent in plaintext but cannot be encrypted.

GeoNetworking packets might be routed via multiple hops. Therefore the radius of received information stored in the Local Dynamic Map might increase significantly.

B.4.4 GeoNetworking Threat Analysis

B.4.4.1 General Assumptions

The suggested countermeasures described in clause 11 are assumed to be deployed. More specifically, it is assumed that an authentication is generated by the originator ITS-S over the packet (i.e. over the payload, common header and extended header), that the final receiving ITS-S is enabled to perform a verification, but that intermediate ITS-S do not perform cryptographic operations. Also the originator is able to encrypt the payload data.

B.4.4.2 Attacks

B.4.4.2.1 General

In an ITS environment, attacks aim at the following:

1) Lower system acceptance (e.g. by repeated false alarms).

2) Endanger safety (e.g. by injecting false packets).

3) Manipulate traffic flow (e.g. by re-routing traffic).

GeoNetworking provides additional attack paths in terms of availability, integrity, confidentiality, and privacy. The corresponding attacks paths are described below.

B.4.4.2.2 Availability

A1: Packets are not forwarded by forwarding ITS-S: restrict or stop information flow.

A2: Packets are forwarded that were not supposed to be forwarded: waste channel bandwidth and computational resources of receiver.

A3: Denial-of-service attacks are amplified:

A3.1:Communication channel is congested outside of local transmission range.

A3.2:Computational resources are wasted outside of local transmission range.

B.4.4.2.3 Integrity

I1: Common header is altered and location and routing table entries of neighbors are falsified.

NOTE 1: The extended header is assumed to be protected by applying the countermeasures described in clause 11.

NOTE 2: This attack could also be classified as availability attack. The attack targets availability by violating integrity.

B.4.4.2.4 Confidentiality

Packets from distant locations are collected by attacker:

C1: Man-in-the-middle actively routeing packets to attacker to gain access to confidential information such as payment, preferences, certification validity time, pseudonym change rate, etc. This attack can also be carried out using a Trojan as the attack proxy.

C2: Collect confidential information from data packets before forwarding (packets not addressed to the forwarding ITS station).

B.4.4.2.5 Privacy

Packets from distant locations are collected by attacker:

P1: Search for location-information to deduce the location or route taken by a specific ITS station. A mechanism is provided to acquire the location of an ITS-S inputting the GeoNetworking address. This mechanism is designed for unicast communication.

P2: Man-in-the-middle actively routing packets to attacker to gain knowledge of identify, location and direction of a specific ITS station. This attack can also be carried out using a Trojan as the attack proxy.

P3: Collect privacy related information such as identity, behavior related information, direction, location, etc. from data packets before forwarding (packets not addressed to the forwarding ITS station).

NOTE: Attacks P2 and P3 equal attacks C1 and C2 but are mounted for different reasons.

B.4.4.3 Security Risks of GeoNetworking

The threat groups and vulnerabilities described in clause 10 also apply to geonetworking. The security risk evaluation is performed for the attacks arising of introducing GeoNetworking.

Table B.2: Risk Determination in GeoNetworking

Threat Group	Applicable Attack	Attack					Impact	Risk
		Factor	Range	Value	Potential	Likelihood		
Availability: Denial of access to incoming packets	• A1 • A2 • A3.1	Time	≤ 1 week	1	7 (Moderate)	2 (Possible)	4 (High)	8 (Critical)
		Expertise	Proficient	2				
		Knowledge	Public	0				
		Opportunity	Easy	1				
		Equipment	Specialized	3				
Availability: Denial of access to outgoing packets	• A2 • A3	Time	≤ 1 week	1	7 (Moderate)	2 (Possible)	4 (High)	8 (Critical)
		Expertise	Proficient	2				
		Knowledge	Public	0				
		Opportunity	Easy	1				
		Equipment	Specialized	3				
Availability: Denial of access to internal resources	• A2 • A3.2	Time	≤ 1 week	1	7 (Moderate)	2 (Possible)	4 (High)	8 (Critical)
		Expertise	Proficient	2				
		Knowledge	Public	0				
		Opportunity	Easy	1				
		Equipment	Specialized	3				
Integrity: Modification and deletion of stored information	• I1	Time	≤ 1 month	4	13 (Moderate)	2 (Possible)	4 (High)	8 (Critical)
		Expertise	Expert	5				
		Knowledge	Public	0				
		Opportunity	Easy	1				
		Equipment	Specialized	3				
Integrity: Modification and deletion of transmitted information	• I1	Time	≤ 1 week	1	10 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
		Expertise	Expert	5				
		Knowledge	Public	0				
		Opportunity	Easy	1				
		Equipment	Specialized	3				

Threat Group	Applicable Attack	Attack					Impact	Risk
		Factor	Range	Value	Potential	Likelihood		
Privacy: Acquisition of personal information	• C1	Time	≤ 1 day	0	7 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	• C2	Expertise	Layman	0				
	• P1	Knowledge	Public	0				
	• P2	Opportunity	Moderate	4				
	• P3	Equipment	Specialized	3				
Privacy: Acquisition of behavioral details	• P1	Time	≤ 1 day	0	9 (Moderate)	2 (Possible)	7 (High)	14 (Critical)
	• P2	Expertise	Proficient	2				
	• P3	Knowledge	Public	0				
		Opportunity	Moderate	4				
		Equipment	Specialized	3				
Privacy: Acquisition of location information	• P1	Time	≤ 1 day	0	7 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	• P2	Expertise	Layman	0				
	• P3	Knowledge	Public	0				
		Opportunity	Moderate	4				
		Equipment	Specialized	3				

B.4.5 Countermeasures

B.4.5.1 General

The previous risk analysis concludes that all attacks impose high (critical) risk. Therefore potential countermeasures will be suggested to counter all attacks A1 - A3, I1, C1 - C2 and P1 - P3. At this time, potential countermeasures are displayed that at a later time will be defined as required, optional, or discarded.

B.4.5.2 Security Design Premise

The selected countermeasures should not enable large-scale denial-of-service attacks (i.e. attacks outside of attacker's transmission range) that cannot be mounted without the selected countermeasures being in place.

B.4.5.3 List of Countermeasures

B.4.5.3.1 Overview

Table B.3 lists potential countermeasures to protect against the threats listed in Table B.2.

Table B.3: Potential Countermeasures

Countermeasure #	Countermeasure	Threats	Risk
C1	Consistency check, incoming plausibility check, and global misbehavior detection	Availability: Denial of access to incoming packets/Denial of access to outgoing packets	Critical
		Integrity: Modification and deletion of transmitted information	Critical
C2	Restrict maximum range and maximum number of hops a packet is routed	Availability: Denial of access to incoming packets/Denial of access to outgoing packets	Critical
		Privacy: Acquisition of personal information, behavioral details, and location information	Critical
C3	Restrict frequency to send messages	Availability: Denial of access to incoming packets/Denial of access to outgoing packets	Critical
		Privacy: Acquisition of personal information, behavioral details, and location information	Critical
C4	Verify (forwarding ITS-S) packet payload on demand	Availability: Denial of access to internal resources	Critical

Countermeasure #	Countermeasure	Threats	Risk
C5	Optionally encrypt packet payload in an end-to-end manner	Privacy: Acquisition of personal information, behavioral details, and location information	Critical
C6	Always sign (original sender and forwarding ITS-S) common header and verify (forwarding ITS-S and final receiver ITS-S) common header on demand	Integrity: Modification and deletion of stored information	Critical

B.4.5.3.2 C1: Consistency check, incoming plausibility check and global misbehavior detection

Misbehavior detection is based on two components and should be strengthened by a third one: local misbehavior detection runs in a receiving ITS-S, global misbehavior detection runs in a central server, and a plausibility check runs in the sending ITS-S:

- Consistency check (runs on sender ITS-S): the consistency check makes sure that the sending ITS-S detects a defect and improper payload data before sending a spurious packet (proper signature but flawed payload). For instance, the consistency check will make sure that the message content does not violate the physical model of the ITS-S (such as unrealistically high speed).

- Incoming plausibility check (runs on receiving ITS-S): the incoming plausibility check detects suspicious packets and reports suspicious behavior to the central authority. Suspicious behavior is any behavior that does not comply to expected behavior, based on direct evidence and probabilistic models. It includes spurious (proper signature but flawed payload) and bogus packets (flawed signature). For instance, direct evidence is given if a vehicle in the neighborhood use the same pseudonym with rapidly switching locations. Evidence based on a probabilistic model is given if an expected behavior does not occur, e.g. if after an emergency brake notification the driver does not react. The local misbehavior detection might also forward random packets to the authorities.

- Global misbehavior detection (runs on central authority server): the global misbehavior detection makes the final decision about misbehaving ITS-S and revokes the credentials of misbehaving ITS-Ss. The global misbehavior detection uses direct evidence and probabilistic evidence to recognize misbehavior. Direct evidence is given if information contradicts physical rules (e.g. two pseudonyms are used at the same time in different locations). Probabilistic evidence is provided if actual behavior derives from expected behavior. The global misbehavior detection might use the same detection mechanisms as the local misbehavior detection, but the available data base is global.

NOTE: The incoming plausibility check and global misbehavior detection will depend on and impact national privacy regulations, system management, and channel congestion. Therefore this countermeasure might be expressed as guidance.

The plausibility check directly counters availability (denial-of-service) attacks and the global misbehavior detection provides deterrence against availability attacks. It counter attacks A1 (observer recognizes that a packet was not forwarded) and A2 (receiving ITS-S recognizes that a received packet was not supposed to be forwarded), and it can also counter attacks A3, P1 and P2 by observing unusual high channel congestion in single local areas or by observing repeated packets of unusual high range. The incoming plausibility check also counters attack I1:

- Countermeasure strategy:
  - Asset hardening and redesign.
- Advantages:
  - Denial-of-service attacks and privacy related attacks in GeoNetworking configuration can be greatly reduced.
- Disadvantages:
  - Introduces bandwidth overhead for communication between ITS-S and central authority.
  - Proper mechanisms to detect misbehavior in the first place are not available yet.

- Implications on ITS architecture:
    - Requires a central authority that is able to make a final decision whether an ITS-S should be revoked.
- Implications on BSA:
    - None.
- Ability to remove relevant ITS problem areas:
    - Denial of service attacks.
    - Long-range denial-of-service attacks.
    - Long-range privacy related attacks.

B.4.5.3.3 C2: Restrict maximum range and maximum number of hops a packet is routed

A powerful attack in GeoNetworking arises by the potential possibility of introducing packets that travel a long distance and many hops. Such attacks can be used to compromise privacy and mount availability attacks. Therefore it appears reasonable to restrict the maximum range of packets, either in terms of hops or geographic location, and also to restrict the maximum size of a geographic target location. A maximum range should be defined system wide and it might be further restricted by each application definition. The application restriction might be a function over variable input (e.g. node density) rather than a fixed number. Also different roles (empowered by permissions expressed in the certificate) might be enabled to use role specific ranges. This mechanism counters attacks A3, C1, P1 and P2.

NOTE 1: The attack to privacy using a request for a geographic location is restricted by this countermeasure. Also using this service to mount a denial-of-service attack by flooding the channel with location requests is countered. Further restrictions of this service might be applied.

NOTE 2: The maximum number of hops is included in the common header and decremented by each intermediate node. Therefore it needs to be considered together with Countermeasure C6 (signature over common header). The geographical location is an absolute value that is not modified by intermediate nodes. If Countermeasure C6 is not applied and the number of remaining hops is sent unprotected, the maximum range of a packet has to be included.

- Countermeasure strategy:
    - Asset hardening.
- Advantages:
    - Large-scale distant attacks are limited.
- Disadvantages:
    - Maximum range needs to be defined wisely.
- Implications on ITS architecture:
    - Maximum range needs to be defined wisely for each application and each role.
- Implications on BSA:
    - Information can only travel a limited range.
- Ability to remove relevant ITS problem areas:
    - Large-scale remote denial of service attacks.
    - Large-scale remote privacy related attacks.

B.4.5.3.4 C3: Restrict frequency to send messages

An attacker mounting a denial-of-service attack likely will broadcast a large number of packets. To counter this attack, the number of allowed transmissions might be restricted. Therefore each ITS-S should count the number of received packets per neighbor and per time unit. An advanced mechanism will be able to detect a change of pseudonyms of a sender and continue the counter properly thereafter. This mechanism counters attacks A3, C1, P1 and P2:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Large-scale distant attacks are limited.
- Disadvantages:
  - Requires computational resources and memory storage.
- Implications on ITS architecture:
  - None.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - Large-scale remote denial of service attacks.
  - Large-scale remote privacy related attacks.

B.4.5.3.5 C4: Verify (forwarding ITS-S) packet payload on demand

An attacker might assemble spurious (proper signature but flawed payload) and bogus packets (flawed signature). GeoNetworking introduces multi-path routing. If an ITS-S does not forward a spurious or bogus packet, this packet might still spread due to the multi-path routing. Therefore it is suggested that forwarding (intermediate) ITS-Ss verify and validate the packet payload. To keep performance demands low, it is suggested that such ITS-Ss verify and validate packets on demand. A minimum rate of packets that needs to be validated and verified should be defined since a very low rate of verifications might lead to spread of bogus and spurious packets due to multi-path routing. This mechanism counters attack A3:

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Remove bogus and spurious packets early.
- Disadvantages:
  - Increases computational demands.
- Implications on ITS architecture:
  - ITS-S might require more powerful controllers.
  - On-demand mechanism involves application layer.
- Implications on BSA:
  - Safety needs to be ensured in face of computational resources bottleneck.
- Ability to remove relevant ITS problem areas:

  - Reduce impact of bogus and spurious packets.

B.4.5.3.6 C5: Optionally encrypt packet payload in an end-to-end manner

GeoNetworking provides several modes, including point-to-point and point-to-multipoint. Data *can* be encrypted to provide privacy and confidentiality in an end-to-end manner if the application wants to protect the payload data. In case of point-to-point, an encryption mechanism such as ECIES with multiple receivers can be used.

NOTE: Encryption does not apply to GeoBroadcast and GeoAnycast. Encryption counters attacks C1, C2, P1, P2 and P3.

- Countermeasure strategy:
  - Asset hardening
- Advantages:
  - Provide confidentiality and thus privacy.
- Disadvantages:
  - Increases computational demands.
  - Only available if destination receiver is known by identity:
    - Point-to-point.
    - Point-to-multipoint.
- Implications on ITS architecture:
  - Time stamp and/or sequence number need to be included in extended header in plain text.
- Implications on BSA:
  - None.
- Ability to remove relevant ITS problem areas:
  - Remove sniffing attacks.

B.4.5.3.7 C6: Always sign (original sender and forwarding ITS-S) common header and verify (forwarding and final receiver ITS-S) common header on demand

The original sender signs the extended header. The original sender and any forwarding node might also sign the common header. This countermeasure makes sure that manipulation of the common header is detected. It also makes sure that manipulation of the common header can be reported under the framework of misbehavior detection, thus providing deterrence to manipulation. This mechanism counters attack I1.

Proposed change to GeoNetworking design: the extended header should contain only data that will not be changed by intermediate ITS-Ss. The common header contains data, that might be changed by intermediate ITS-Ss. For instance, the target location might be set by the original sender in the extended header and then refined by intermediate ITS-S in the common header.

The required computational resource overhead is considerable and an alternative mechanism is the following:

- Do not sign common header (i.e. do not apply Countermeasure C6).
- Perform plausibility check over common header.

NOTE 1: If Countermeasure C6 is not applied, the common header should be signed together with the payload and extended header by the originator.

NOTE 2: If countermeasure C6 is not applied, the number of remaining allowed hops will be sent unprotected (see Countermeasure C2).

NOTE 3: The impact of not using countermeasure C6 requires further research.

- Countermeasure strategy:
  - Asset hardening.
- Advantages:
  - Remove packets with flawed common header.
  - Avoid misinformation in LDM.
- Disadvantages:
  - Increases computational demands heavily.
- Implications on ITS architecture:
  - ITS-S might require more powerful controllers.
  - On-demand mechanism involves application layer.
- Implications on BSA:
  - Safety needs to be ensured in face of computational resources bottleneck.
- Ability to remove relevant ITS problem areas:
  - Increase trustworthiness of information stored in LDM.

B.4.5.4 Further Countermeasures

Further countermeasures that were introduced in clause 11 should also be used for GeoNetworking. These include (without being complete):

- Signature and verification of packet payload and of extended header.
- Using pseudonyms and regularly changing all identifiers at the same time.
- Minimize any information that can be used for identification (e.g. measurement units).
- Replay protection with time-stamp and sequence numbers.
- Assurance level based on certificate attributes and confidence level based on local misbehavior detection evaluation.

B.4.6 Incentive Schemes

Incentive schemes provide incentives to forwarding nodes. Incentive schemes avoid selfish behavior of stations to save resources. In ITS, selfish nodes save computing resources (less cryptographic operations) and in case of handheld devices ITS-S save energy resources (battery charge).

In case of a "typical" ITS-S attacker, the attacker will focus on DoS attacks (wasting other node's resources and availability) rather than saving own resources. Selfish behavior is expected to be less dominant and malicious behavior will be dominant. Hence, incentive schemes are not considered here.

B.4.7 Security Performance

B.4.7.1 General

The described security mechanisms increase channel and computational resources requirements. The *additional* security overhead is listed below and lower layer overhead are neglected. Only elliptic curve operations are included and further cryptographic operations including hash and symmetric encryption is neglected.

To keep security performance demands low, it is suggested to perform signature verification on-demand only. This holds for the packet payload (see Countermeasure C3) and the packet common header (see Countermeasure C5).

B.4.7.2 Confidentiality (Countermeasure C5)

Table B.4 describes the performance for Countermeasure C5.

Table B.4: Performance for Confidentiality

Field for list of ECIES encrypted key	• 12 bytes AES-CCM nonce (per message) • around 73 bytes per receiver: (33 bytes point, 16 bytes encrypted key, 16 bytes HMAC, 8 bytes receiver identifier)
ITS-AID + SSP	at least 1 byte
Encrypted data	payload + CCM authentication tag (16 bytes)
TOTAL Channel Overhead	#receivers x 73 + 12 + 1 + 16 bytes ≥ **102** bytes
TOTAL Computational Overhead	• Original Sender: one ECIES encryption per receiver + one AES-CCM encryption over payload • (Each) Final Receiver: one ECIES decryption for key + one AES-CCM decryption over payload

B.4.7.3 Integrity (Countermeasures C4 and C6)

Table B.5 displays the performance for integrity.

Table B.5: Performance for Integrity

Field for ECDSA Signature for common header, extended header, and payload	64 bytes
Field for sender's certificate	around 140 bytes
ITS-AID + SSP	at least 1 byte
TOTAL Channel Overhead	64 + 140 + 1 = **205** bytes
TOTAL Computational Overhead	• Original Sender: [one ECDSA signature over common header, extended header, and payload] • (Each) Forwarding ITS-S: [p x one ECDSA verification over common header, extended header, and payload] + [p x one ECDSA verification for original sender's certificate] • Final Receiver: [one ECDSA verification over common header, extended header, and payload] + [one ECDSA verification for original sender's certificate]
NOTE 1: The underlined operations only needs to be performed once per sender's pseudonym. NOTE 2: p describes probabilities between 0 and 1 that represent the verify-on-demand ratio.	

B.4.7.4 Confidentiality + Integrity (Countermeasures C4, C5 and C6)

If encryption and authentication is applied at the same time, the channel overhead and computational overhead need to be accumulated and there are no savings and overlappings.

History

Document history		
V1.1.1	March 2010	Publication
V1.2.1	March 2017	Publication