ESPR: Efficient Security Scheme for Position-Based Routing in Vehicular Ad Hoc Networks

by

Nizar Alsharif

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2010

© Nizar Alsharif 2010

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Vehicular Ad hoc Network (VANET) is a promising emerging technology that enables road safety, traffic management, and passengers and drivers comfort applications. Many applications require multi-hop routing; position-based routing (PBR) is a well-recognized routing paradigm that performs well in the vehicular context to enable these applications. However, there are many security challenges and various routing attacks which may prevent the deployment of PBR protocols.

In this study, we propose a novel security scheme called ESPR to secure PBR protocols in VANETs. ESPR considers both digital signature and keyed Hash Message Authentication Code (HMAC) to meet the unique requirements of PBR. In ESPR, all legitimate members share a secret key. ESPR scheme applies a novel probabilistic key distribution to allow unrevoked members to update the shared secret key. Furthermore, it defines a set of plausibility checks that enables network members to detect and avoid PBR attacks autonomously. By conducting security analysis and performance evaluation, ESPR scheme demonstrated to outperform its counterparts in terms of communication overhead and delay while achieving robust and secure operation.

Acknowledgements

All praises are due to Allah for giving me the ability to write this work. All praises are due to Allah for giving me the honor of helping the humanity by contributing to enrich its knowledge.

I would like to express my deepest appreciation and gratitude to my supervisor Professor Xuemin Shen for his continuous guidance, support, patience, and encouragement. The experience that I gained while working under professor Shen's supervision has not only developed my academic skills, but it also refines my character.

This thesis would not have been possible without the assistance of many people. I would like to express my extreme appreciation to Albert Wasef for his assistance and cooperation to make this work possible. My regular discussion meetings with Albert have helped me to explore the research area and provide me many inspirations in my work. Also, I want to thank my colleagues at the broadband communication research (BBCR) group, and the security and privacy group.

Special thanks to the Ministry of Higher Education in Saudi Arabia and the Saudi Arabian Cultural Bureau in Canada for their financial and academic support.

I would like also to thank all my friends in University of Waterloo who have made Waterloo such a great place to live. Special thanks to Waleed Alasmary, Mazen Alsabaan, Abdullah Bin Humayd, Omar Binhomaid, Mohammed Bait Suwailam, and all my friends, who make my life colorful and enjoyable.

I am truly indebted to my parents, my in-laws, and my sister Sahar for their endless support, encouragement, prayers, and love.

Amani, my dear wife, is always my source of inspiration. I owe Amani my deepest gratitude for her infinite patience that accompanies me along this long journey to fulfill

my goals. Amani and my daughter Jolie are my source of strength. Their love is my motive, and their happiness is my ultimate goal.

To my beloved wife, Amani Alfageah

Contents

List of Tables

List of Figures

List of Algorithms

Chapter 1

Introduction

Vehicular Communication Systems (VCSs) are an emerging technology that employ wireless communication networks to enable vehicles to communicate with one another, and with a fixed infrastructure. VCSs are a direct response to the increasing demands of Intelligent Transportation Systems (ITS) services and the expectations of the automotive industry. Vehicular communication is designed for a wide range of applications related to safety, traffic management, and passenger comfort.

Safety applications are the main motivation for the development of VCSs. VCSs are used with the goal of spreading accurate data quickly and reliably, in order to avoid accidents and loss of life. In VCSs, vehicles help to avoid accidents through cooperation: they inform one another about their own source-of-risk behaviour, such as highway merging, they also disseminate emergency warning messages when a hazardous status is detected, such as slippery road conditions. A VCS also improves road safety by enabling traffic lights and signs to communicate with vehicles.

In addition to these safety applications, VCSs are also employed in a variety of ITS traffic management applications. Road traffic management applications focus on improving traffic flow in order to avoid traffic congestion, to reduce travel time, and to utilize

the transportation infrastructure effectively. Examples include adaptive traffic lights that change according to the status of the traffic in an intersection, and direction information based on real-time traffic information.

A third type of VCS applications relates to the comfort and well being of passengers; transferring files between vehicles, accessing the Internet during trips, finding a nearby point of interest, and disseminating advertising messages about a nearby business are all examples of VCS services. These services have been included in response to passenger, car manufacturer, or service provider requests.

Vehicular networks have attracted the attention of both research and industrial communities, which is reflected in the interest of governments and standardization organizations. For example, European car manufacturers have instituted the Car-to-Car Communication Consortium (C2C-CC) [1] to improve road safety and efficiency, and the U.S FCC (Federal Communication Commission) has approved a 75 MHz spectrum for vehicular networks [2]. The Institute of Electrical and Electronics Engineers (IEEE) also supports vehicular communication with the IEEE 1609 family of standards for wireless access in vehicular environments (WAVE) [3].

The previous works present a variety of approaches that employ various technologies for the implementation of VCS. In fact, some car manufacturers support their vehicles through Internet access via cellular networks. However, with respect to cost and latency, using cellular networks is not the best way to build a VCS. In many proposals, IEEE 802.11 is deployed for a VCS. However, IEEE 802.11 has a limited radio range and needs numerous base stations to keep the vehicles connected to the infrastructure. Using Vehicular Ad Hoc Network (VANET) with On-Board Units (OBUs) and Roadside units (RSUs), and enabling multi-hop routing through vehicles appears to be the more effective method, but it also entails significant challenges.

1.1 Research Motivations and Objectives

Security is a major challenge that can affect VANETs deployment. As a special case of mobile ad hoc networks (MANETs), VANET inherits all of MANETs security concerns while introducing new security challenges specific to its characteristics. In VANETs, attackers can inject, forge, replay, and drop messages in order to violate information integrity, authenticity, user privacy, and system performance. Therefore, reliable security solutions should be designed to achieve user authentication, information authentication (data integrity), and non-repudiation, which are identified as primary security requirements.

Multi-hop routing is a key function in VANET. The literature shows that position-based routing (PBR) outperforms other routing schemes in the vehicular context. However, PBR protocols are vulnerable to many routing attacks, such as: routing loop, sinkhole, wormhole, and sybil attacks. Routing attacks can be launched even when the security requirements are met; therefore, security protocols should consider these attacks in their design.

In literature, public key infrastructure (PKI) has been adopted in the vehicular communication environment in order to meet security requirements. However, applying a PKI scheme into the PBR context is more challenging, because PBR packets have two types of data fields: mutable and immutable fields. Neither hop-by-hop nor end-to-end digital signature-based authentication is sufficient to secure the multi-hop routing process. Security protocols should be carefully designed to secure PBR services.

The most noticeable work that addresses the PBR security problem considers a scheme with two digital signatures on each packet, in order to secure both mutable and immutable data fields [4]; however, this scheme fails to meet the hard delay constraint for some VANET's applications, and introduces a high communication overhead to the network. It is important to consider these two constraints in order to design an efficient security

protocol.

1.2 Research Contributions

In this thesis, a comprehensive solution is provided to secure PBR protocols in VANETs. The major contributions are:

- Identifying PBR security challenges and attacks
- Identifying PBR security requirements
- Proposing a cryptographic security scheme to achieve, efficiently, the primary security requirements
- Proposing a corresponding key management scheme to manage secure distribution, revocation, and key renewal processes
- Evaluating the impact of different routing attacks on the network performance
- Proposing a plausibility-checks set in order to enable vehicles to detect and avoid malicious behaviours autonomously

1.3 Thesis Organization

The remainder of this thesis is organized as follows: Chapter 2 presents an introduction to VANETs and PBR, a literature review of their security systems, and recent related work; Chapter 3 defines the proposed security scheme, ESPR; Chapter 4 presents a security and efficiency analysis of ESPR, in addition, it includes a simulation-based performance evaluation of ESPR; and Chapter 5 summarizes the thesis, as well as commeting the major contribitions, and outlining some feasible future work.

Chapter 2

Background and Literature Review

2.1 Vehicular Ad Hoc Network

Vehicular Ad Hoc Network (VANET) is an emerging wireless ad hoc network that enables vehicular communication. In general, Ad-Hoc networks are decentralized networks that do not depend on preexisting infrastructure, e.g., routers, and the routing process is dynamic where each node participates in routing. In VANETs, each vehicle is equipped with a networking device, On-Board Unit (OBU), to enable V2V. Similar devices, Roadside units (RSUs), are spread along the road sides to allow V2I. Figure 2.1 shows the general structure of VANET.

In addition to general wireless and ad hoc characteristics, such as decentralizing and short transmission range, VANET also has its distinctive characteristics. VANET is a large-scale network characterized as a network that is frequently disconnected or partitioned, and that has a highly dynamic topology due to the high level of mobility of the vehicles. However, in VANET, the mobility of the vehicles can be modeled and predicted because vehicle movements are constrained by streets and roads. Two main entities comprise VANETs: OBUs and RSUs that have sufficient computation, energy, and storage

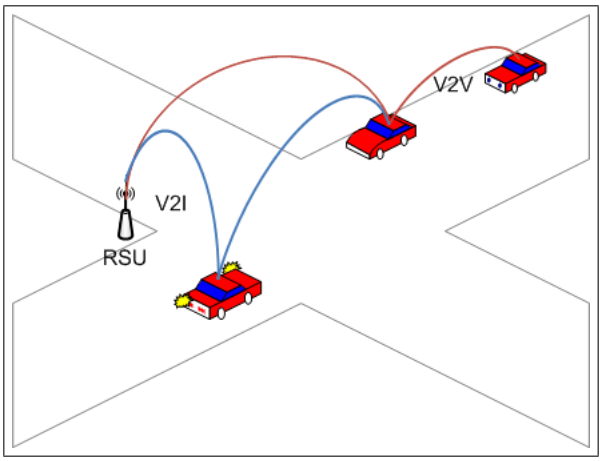
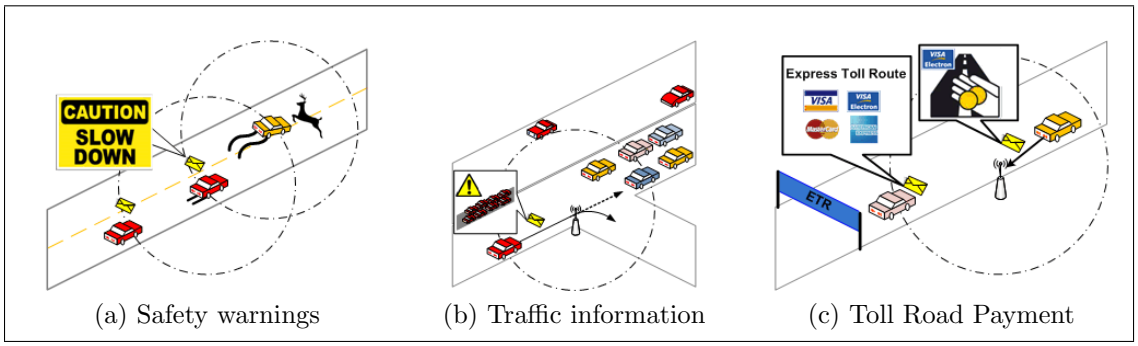


Figure 2.1: Structure of VANET

capabilities. Moreover, VANETs have hard delay constraints, specially for safety applications. These characteristics make VANET a unique class of networks; however, they also introduce many challenges that must be resolved.

The first challenge is network reliability because the highly dynamic nature of the topology of a VANET threatens its reliability. Achieving reliable communication requires an efficient medium-access control (MAC) protocol that can adapt to a VANET environment in terms of mobility and interoperability. In addition, efficient routing protocols and dissemination algorithms are needed in order to deal with such a large-scale, frequently partitioned network that has different applications with different priorities for different vehicles densities.

Security is another key challenge. Solutions are required to ensure secure communication between legitimate vehicles and authorized services while having little or no impact on the ease-of-use of the services. Security solutions should be acceptable to users, e.g., drivers, car manufacturers, and service providers, with respect to cost, overhead, and efficiency. Moreover, the overhead provided by security solutions should not violate the latency constraint of a VANETs applications.



(a) Safety warnings (b) Traffic information (c) Toll Road Payment

Figure 2.2: Examples of VANET applications

VANET is thus a promising network that is expected to revolutionize transportation systems and society by enabling remarkable applications with respect to safety, traffic management, business services, passenger comfort, and other areas. Some of the VANET applications are shown in Figure 2.2. However, its unique characteristics give rise to many challenges related to its commercialization. The lack of a fixed infrastructure and the high mobility of the vehicles are the properties that require the most extensive effort in order to solve problems related to communication reliability, packet routing, and network security.

2.2 Position-Based Routing (PBR) in VANET

Routing is one of the key enabling mechanisms for multi-hop applications in VANETs. However, due to vehicles high degree of mobility, designing an efficient routing protocol for VANETs is very challenging. The traditional topology-based protocols and source routing protocols, such as AODV [5]and DSR [6], require finding routes and maintaining routing tables and do not perform well with the highly dynamic topology of VANETs. Position-based routing (PBR) is a promising routing paradigm, which depends on the availability of geographic location information about the vehicles. Since each vehicle in VANET is equipped with a Global Positioning Systems (GPS) receiver, it can accurately determine its geographic location. Studies show that PBR outperforms topology-based routing in

urban and highway scenarios[7].

Vehicular communication projects such as CarTalk2000 [8] and NoW [9] have introduced PBR to cope with a vehicular network environment. PBR is suitable for VANET as it does not require prior determination of a routing path. In PBR, each vehicle is aware of its own geographical location. Nearby vehicles share this location information in order to perform data routing. A routing decision is determined at each intermediate node with respect to the position of the destination, the position of vehicles within the transmission range (neighbour nodes), and the forwarding strategy of the protocol. PBR protocols thus consist of the following components:

- Beaconing: Each vehicle should periodically broadcast its geographic location and identity. Based on the beacons received, each vehicle maintains a table of the locations of the neighbouring vehicles.

- Location service: Before a vehicle can send a message to another vehicle, it should determine the geographic location of the destination vehicle through location queries and responses. A location query that includes the identity of the destination is broadcast by the source vehicle in a well-defined manner (e.g., it is rebroadcast until a maximum number of hops is reached). The source waits until it receives a location response that provides the updated location of the destination. The location reply can be generated either by the destination itself or by a location server.

- Forwarding strategy: Forwarding a message from node to node in PBR follows a forwarding strategy. Different PBR protocols operate according to different strategies and consider a variety of information required by their specific strategy. For example, Greedy Perimeter Stateless Routing (GPSR) [10], one of the fundamental PBR protocols, combines greedy routing with face routing as forwarding and recovery strategies. In greedy forwarding, packets are forwarded to the vehicle with the

physical location closest to the destination. However, when greedy fails and reach a local minimum, face routing, or perimeter algorithm, is used. GPSR requires only the positions of the destination and the neighbouring vehicles, while other protocols may employ map information, traffic density information, the trajectories of the vehicles, information about speed and direction, etc., in their forwarding strategy.

The routing header of a packet in PBR should include the identity, timestamp, and position of the source, destination, and sender vehicles, where the source and destination are the end nodes, and the sender is the last intermediate packet-forwarder. PBR supports unicast and geocast message forwarding Figure 2.3 shows two examples of PBR routing packets, where the routing header consists of two types of fields: immutable which are not modifiable by intermediate nodes, and mutable which are modifiable by intermediate nodes. In geocast message forwarding, the destinations identity is replaced by the geographic coordinates of the targeted area.

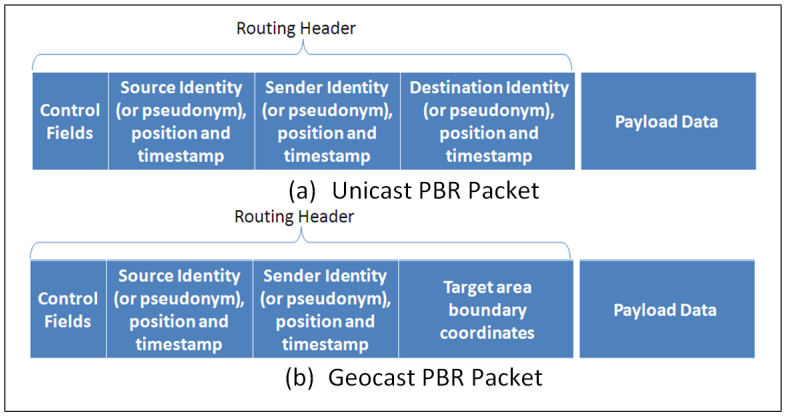


Figure 2.3: Examples of Position-Based Routing Packets

When a vehicle wants to send a message to another vehicle, it determines the position of the destination vehicle through location services. Then, the source vehicle, based on the stored location table for the neighboring vehicle, forwards the message to the next vehicle according to the routing protocol forwarding strategy. This process continues until the

message reaches its destination.

2.2.1 PBR Protocols

Many PBR protocols have been proposed for mobile ad hoc networks (MANETs). These protocols can be classified into three main categories [7]. The first category includes directional flooding protocols, according to which packets are flooded on multiple paths restricted by a defined area. For example, Location Aided Routing (LAR)[11]was one of the first PBR protocols that floods packets in a rectangular zone that extends from the source to the destination. The second class of PBR protocols uses hierarchical approaches in their forwarding strategy. Terminodes[12] and grid routing [13] are examples of these protocols. The last category is greedy routing, whereby packets are forwarded on only a single path and nodes are selected according to the closest-to-the-destination rule. Most PBR protocols proposed for VANET belong to this category.

Greedy routing suffers from the local minimum problem. GPSR [10] solved this problem by combining greedy routing with face routing and provided successful results in open area simulations. However, GPSR has many problems and fails in some situations. Fan Li and Yu Wang discuss some of these situations in [7]. Greedy Perimeter Coordinator Routing (GPCR) [14] is another greedy protocol that relies on routing at junctions; its forwarding strategy depends mainly on the fact that vehicles at junctions follow a natural planar graph. Because it uses greedy routing, GPCR employs a repair strategy in order to avoid the local minimum problem. Geographic Source Routing (GSR)[14] is an anchor-based source routing protocol. The destination location is determined, and the best route is then computed in the form of a route vector that contains a list of anchors or fixed geographic points between the source and the destination. Packets are forwarded from one anchor to another using a greedy scheme until the packet is received by the destination.

Spatial Awareness Routing (SAR) [15] is a map-based source routing protocol. SAR

depends on a GSR protocol whereby the best route is selected with respect to the city map, and the path in the form of selected junctions is attached to each packet, which is finally forwarded from one node to another using GSR. Connectivity Aware Routing (CAR) [16] is a similar protocol that adds a connectivity maintenance stage to the routing scheme. As with SAR, CAR first determines the destination location and then attaches a proper path to the header for each packet. During the stage in which the route is computed, this protocol broadcasts short messages in order to discover connectivity, and it also uses velocity vector information.

Position-based protocols that use traffic information give better levels of performance: higher delivery rates and relatively less delay. Traffic information helps vehicles predict the density of the nodes and the partitioning of the network along a variety of routes. A-STAR [17], MDDV [18], and SADV [19] are examples of this type of protocol. A-STAR (Anchor-based Street and Traffic-Aware Routing) combines both SAR for awareness and Global State Routing (GSR) for routing. It uses traffic density information to add weights for path selection based on the premise that more traffic leads to better network connectivity. In addition, it suggests a strategy for avoiding the packet reaching nodes with no neighbours (local optimum) by marking such a specific street temporarily as a zero-weighted street (out of service).

MDDV (Mobility-Centric Data Dissemination for VANET) is another trajectory-based protocol. It is a geographically opportunistic forwarding scheme based on source node routing. However, the authors of this protocol relied on static network information and assumed that it is very difficult to access real-time traffic information. They use the number of lanes per street in a map as a weighting factor that might indicate traffic density for that street. MDDV uses greedy forwarding in order to forward packets to the next junction and introduces an opportunistic approach in order to achieve a better delivery rate. Every node receives a packet and forwards that packet if it will move it

toward its destination. Each packet includes its generation time and only newer messages are subject to forwarding. SADV (Static Node-Assisted Adaptive Routing Protocol for VANETs) uses static ad hoc nodes at intersections in order to improve the data delivery rate. The roles of these nodes are to store packets temporarily until a vehicle moving toward the destination enters the intersection and to collect real-time information about the density of nodes in different paths in order to make better routing decisions.

In addition to maps and information about node density, some protocols assume that more information is available for vehicle routing, such as velocity vectors. The Motion Vector (MoVe)[20] scheme introduced the idea of benefiting from knowledge of the velocity vector, route, and destination of the carrier vehicle and then, depending on this information, the node (vehicle) determines the best moment to forward the packet to another vehicle that is closer to the destination. A carrier vehicle uses *hello* and *response* messages in order to obtain information about its neighbours. The Geographical Opportunistic routing protocol for VANET (GeOpps) [7] is a recent position-based routing protocol. Based on a concept similar to that in MoVe, it uses geographical information from navigation systems, assumes prior knowledge of a vehicles (carriers) path, and then calculates the best moment to forward the packets. GeOpps employs a delay-tolerant approach, and its delivery rate is better than either the greedy routing or MoVe protocols.

2.3 Security and Privacy in VANET

Providing secure communication is a major challenge in VANET that can impact its deployment. Reliable security solutions are required in order to secure both communication between participants and service access. These security mechanisms should be able to cope with a VANET environment and also be acceptable to VANET participants: passengers, car manufacturers, service providers, etc. Security mechanisms should also be based the

premise that safety information should not be denied to any vehicle but that the system should not be open to alteration or infiltration by an attacker. Another consideration is that some VANET services need to be accessible only to authorized users (e.g., on-road payments).

Cooperative vehicle behaviour is another important concern with respect to VANET security. Because ad hoc networks in general require node cooperation, security mechanisms should be designed to encourage cooperation and to detect any $selfish$ behaviour. In VANET, some vehicles are uncooperative by dropping messages or by not providing their information (e.g., position information in PBR) in order to conserve their resources (computation, power, bandwidth, etc.) or for security and privacy reasons. Privacy is a major concern for drivers and a major challenge for designers. Especially for private vehicles, identity privacy, or anonymity, should be guaranteed. Privacy mechanisms should guarantee that the shared transmitted information does not enable traceability.

Thus, successful deployment of a VANET requires that privacy and security be considered in the design. A comprehensive security architecture is required in order to support VANET at the required level of security without deploying additional infrastructure or disturbing the ease-of-use of its services. Such architecture is expected to ensure that VANET operates efficiently with respect to trust, authentication, access control, robustness, and secure service access while preserving user privacy.

2.3.1 VANET Security and Privacy Threats

As in any other network, message delivery in VANET is vulnerable to security threats. VANET attackers can be described according their attributes: active or passive, internal or external, rational or malicious, and independent or coordinated [2]. The types of attack can also be classified according to the following categories:

- Denial of service (DoS):

  DoS denotes a scenario in which an active attacker tries to bring down the network (or part of it), partition it, make services unavailable, or in some cases, cause accidents. Radio jamming and overwhelming the network by message injection are two examples of DoS attacks. In message dissemination scenarios, dropping packets selfishly is also considered a DoS attack.

- Bogus information dissemination (BID):

  An attacker can send bogus information to clear the road or to create congestion. Falsified warnings, for example, might cause accidents. Many PBR attacks involve the sending of falsified position information, and forged identities are used in impersonation attacks. In BID scenarios, the attacker generates wrong information or replays previous messages.

- Privacy disclosure:

  Privacy issues relate to who is talking to whom, the content of private messages, services being used, sites being visited, and the location of private vehicles. An attacker can listen passively to a channel or actively persuade users to be a part of their communication route, such as with wormhole and sinkhole attacks. The attacker can then eavesdrop on active sessions to extract sensitive information. In addition, monitoring traffic and disclosing the identities of drivers can facilitate their traceability.

2.3.2 PBR Attacks

In PBR-related attacks, the goals of the attacker include creating or avoiding traffic congestion, obtaining privileges that belong to others, causing accidents, or denying service (DoS). Attackers replay, forge, inject, or alter packets in order to achieve their goals. The

following are the primary types of PBR attacks in VANET:

- Routing loop attacks:

  An attacker can launch this attack by taking wrong routing decisions, where it passes the packet back to one of the previous forwarders. Another way to launch this attack is that the attacker forges its position to appear closer to the destination causing other nodes to select the attacker as their next hop. Then, the attacker passes any received packet to one of the previous nodes. The routing loop attack causes the packet to bounce in a loop, and hence, preventing the packet from reaching its destination.

- Wormhole attacks:

  Two attackers can establish a high speed private connection between them to capture packets from one location and replay them in a different location. The aim of the attacker in this attack is dominating the routing paths to drop packets and partition the network or for eavesdropping purposes.

- Sinkhole attacks:

  The attacker claims a different position to appear as the next forwarder to a common target, e.g., an RSU, to dominate the routing path, and then, drops the packets.

- Sybil attack:

  The attacker pretends to be multiple vehicles by sending a variety of bogus beacons. A Sybil attack can be used to create traffic congestion or to divert traffic from the attackers route.

- Impersonation attacks:

  By replaying beacons or forging identities, the attacker pretends to be another vehicle in order to obtain its privileges.

- Packet modification: The attacker changes the content of the packet, e.g., a forwarder changes the destination area of a geocast warning message.

Figure 2.4 shows some examples of PBR attacks.

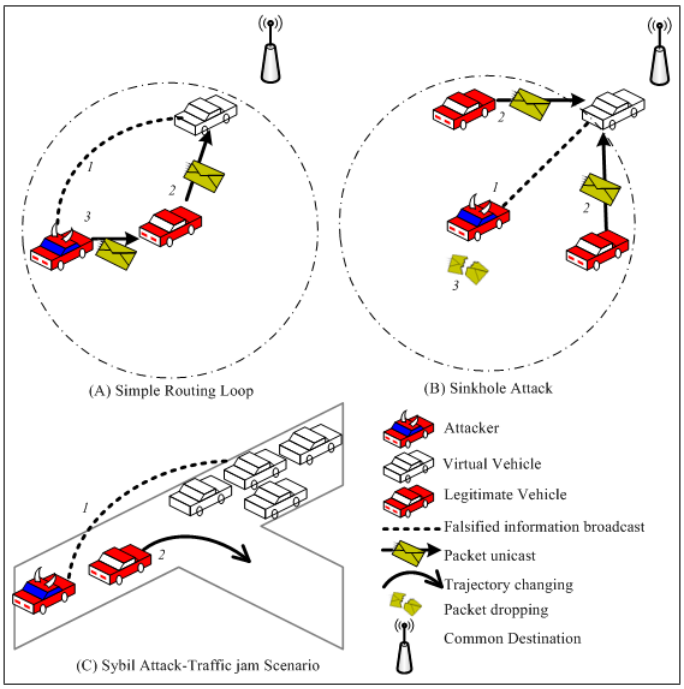


Figure 2.4: Examples of PBR Attacks

2.3.3 PBR Security Requirements

To prevent the potential PBR threats described above, a well-developed security scheme should take into consideration the following requirements:

- Service availability:

  DoS attacks that cause the network to be unavailable must be prevented or at least reported. The PBR security scheme should be able to take into consideration any resource depletion at the routing level, such as a routing loop attack or packet injection attacks.

- Message integrity:

  Messages should be routed without unauthorized modification by an intermediate

forwarder. Mutable fields, which contain the IDs for the current node along with any extra information required by the protocols, should be updated in an authorized manner and delivered unaltered to the next node, while the immutable fields should be delivered to the destination without any modification.

- Source authentication:

  The originator of a message should be legitimate and authentic so that the information delivered can be trusted and impersonation should be impossible. It is not sufficient to ensure only that the origin of the message is a legitimate node. Originator authentication is also required so that any legitimate user can be identified and excluded, based on compromising or inappropriate behaviour (user traceability). Moreover, the routing process should be conducted only among legitimate users in order to enhance delivery and avoid routing attacks.

- Source non-repudiation:

  The originator of a message must be prevented from denying the creation of the message. For example, nodes which cause accidents by disseminating falsified information or by depleting the network should not be able to deny their misbehaviour.

- Protocol efficiency:

  An efficient security scheme should consider both communication overhead, i.e., packet size, and end-to-end latency, and should ensure that VANET constraints are not violated. For example, end-to-end latency has an upper bound of 100 *msec* for safety messages, as identified in [2].

2.3.4 PBR and Privacy

In PBR, nodes periodically send beacon messages that contain their identifiers and precise positions and that breach the privacy of information about their location. Attackers that

are eavesdropping for beacons can then trace a node or a driver. Location services could also be used to disclose locations and violate privacy. Anonymization techniques were proposed early on in order to enhance privacy in mobile ad hoc networks. In VANET, temporary pseudonyms together with the deployment of a public key infrastructure (PKI) have been applied in order to preserve a users privacy, e.g., in [21]. In [22], the impact of pseudonym changes on PBR was investigated. The results of the analysis and simulation show that pseudonym changes affect network performance and increase the packet loss rate, especially with short pseudonym change intervals and scenarios involving low traffic density.

For RSUs along roadsides, fixed service stations, and non-private vehicles, privacy is not an issue. While privacy is a major concern for private vehicle drivers, privacy concerns have not prevented the wide deployment of cellular networks, automatic teller machines (ATMs), and wide acceptance of the Internet [23]. With respect to the promising performance of PBR, some studies consider privacy a secondary requirement and orthogonal to PBR. Thus, while privacy is not highlighted in the current work, privacy schemes could be a complementary aspect.

2.4 Related Work

Security in VANET has attracted a sustained effort from vehicular communication projects, standardization organizations and security researchers. As government-supported consortiums, the CAR 2 CAR Communication Consortium [1] in Europe and DSRC [3] in the United States, in particular the P1609.2 group, have put prominent effort in vehicular communication. Other projects have also contributed to defining security prototypes or providing security solutions. For example, the SEcure VEhicular COMmunication (SEVECOM) project [24] focuses on defining security requirements for vehicular communication

and implementing corresponding solutions. The NoW (Network on Wheels) project [9] is another vehicular communication project interested in data security.

Although a number of studies have been conducted, the domain of VANET security is still young, and many issues are still unresolved. Industrial projects and academic researchers have provided significant contributions. This literature review presents related research to PBR security. Several perspectives are included: the general design of a security scheme that satisfies the security requirements; solving the problem of providing falsified position information in PBR; and securing PBR in VANET.

2.4.1 Security Design

In addition to the standard drafts and commercial projects efforts, a number of studies have significantly enriched the domain of VANET security. Raya *etal.* in [2] and Papadimitratos *etal.* in [4] have presented a wide view of VANET security. They provided threat analysis and adversary models and from them deduced security requirements and security models appropriate for VANET. The results of their work are general, rather than detailed, security and privacy solutions. Comprehensive schemes and frameworks have also been proposed, such as[25], [26], and [4]. Most researchers support a public key infrastructure (PKI) as a method of satisfying the requirements associated with VANET security. Group signatures[26] and pseudonyms [25] have also been proposed as a means of protecting users privacy.

In [25], bilinear mapping is used to implement an efficient pseudonym PKI scheme (EPPKI) in order to provide security and privacy in VANET. With EPPKI, to preserve privacy, each node is supplied with only a master key and a master certificate, from which it then generates traceable pseudonyms and pseudonymous certificates to be included in its communication. The security protocol requires each node to sign each outgoing message

and to verify each incoming message. In other words, EPPKI can be classified as a hop-to-hop authentication scheme, and it fails to address multi-hop routing security.

GSIS [26], also based on bilinear pairing, is another notable comprehensive scheme for safeguarding VANET security and privacy. In GSIS, group signatures for OBUs and identity-based signatures for RSUs have been proposed in order to maintain security and privacy. A message received from an OBU can be verified by its signature; so that the receiver can determine whether that OBU is legitimate. However, coverage of multi-hop routing is also lacking in GSIS.

Other research in this area is devoted mainly to analyzing possible attacks or to addressing particular attacks and providing corresponding security mechanisms. In [2], the focus was on an attacker model and specific VANET attacks. In [27], an attack tree was provided for assessing both hardware and software threats through the communication system NoW. In addition, some studies have provided solutions for specific security issues, such as a Sybil attack or selfish behaviour. Most of the solutions proposed with respect to these two types of attacks are based on cooperative monitoring of node activities and the exchanging of information extracted by means of reputation systems or credit-based mechanisms.

2.4.2 Falsified-Position Countermeasure

Because PBR was proposed mainly for wireless sensor networks and mobile ad hoc networks, many position verification schemes have been developed. In general, position verification methods can be classified as either infrastructure-based and infrastructure-less, autonomous, and cooperative schemes or as schemes that require or do not require dedicated hardware [28]. The schemes that have been developed can thus be described according to some of these attributes.

Most infrastructure-based mechanisms were originally proposed for sensor networks and then deployed for VANET. In these methods, infrastructure devices such as base stations are deployed together with some fundamental rules for positioning for the purposes of verifying locations. Verifiable multilateration [29] and triangulation [30] are examples of this category: the position is determined by the distance measurements between the vehicle and some reference nodes or base stations. The principles on which these schemes are based include the measurement of distance and signal angles based on specified parameters, such as time of arrival, signal strength, and the angle of the signal. These methods introduce additional infrastructure cost to VANET.

In autonomous schemes, each node independently verifies the position claimed by the sender in the packet received. Most autonomous schemes depend on some form of plausibility check in order to guarantee that the position claimed is plausible. For example, plausibility checks have been proposed in [31] and include checking to determine whether the position claimed is within a plausible transmission range and located on a roadway. On the other hand, cooperative schemes require nodes to exchange information with other nodes in order to verify information received about their neighbours position. For example, in [32] two directional antennas are used to locate vehicles positioned in front of the node and behind it. When they share this information, vehicles in the region obtain a more accurate view of the temporary topology. Reputation systems are another form of cooperative scheme cite2010reputation, in which any participating node has a reputational value that increases based on its cooperation with other nodes and decreases when it misbehaves.

2.4.3 Secure PBR for VANET

Only a few studies have addressed the problem of securing position-based routing in VANETs, such as in [4], in which Harsch *etal*. proposed a *hybrid* signature scheme for securing PBR in VANETs by applying hop-by-hop (HbH) and end-to-end (E2E) authenti-

cation together with plausibility checks. In the HbH signature scheme, each node signs the packet and forwards it to the next one. The next forwarder then verifies the senders signature, removes the signature, updates the mutable fields in the header, signs the packet, and resends it. In contrast, an E2E signature scheme does not require the signature of the forwarder: only the originator of a packet signs its immutable fields and forwards it. Every subsequent forwarder verifies the originators signature, updates the mutable fields, and forwards the packet.

An HbH signature scheme is not sufficient for protecting the process of multi-hop routing. HbH does not provide the end receiver with a guarantee of data integrity, source authentication, or nonrepudiation. It also fails to protect the message delivery process from PBR threats such as a sinkhole attack. The E2E signature scheme, on the other hand, does meet the requirements for primary security, data integrity, source authentication, and nonrepudiation. However, an E2E system does not provide security for mutable fields, which makes the scheme highly vulnerable to PBR attacks and selfish behaviour.

For the hybrid signature scheme, the source of the message signs on to both mutable and immutable fields. Each forwarder then verifies the digital signatures of both the originator and the previous forwarder, updates the mutable fields, and replaces the last signature with its own. Used in combination with plausibility checks, this scheme supports PBR protocols with the level of security required because the primary security requirements are satisfied, and packets are forwarded through authentic nodes.

An alternative incremental signature scheme is described in [4], where each intermediate forwarder verifies the previous signatures, copies the mutable field into the end of the packets, updates the mutable fields with the current information, and adds its signature for the whole packet to the signature chain. This strong scheme enables both forwarders and the final destination to obtain a larger view of the network. However, from a network perspective, it adds unnecessary overhead and delay, which may affect the functional-

ity of VANET. Table 2.1 shows the cryptographic operations performed in each of the above schemes: G represents signature generation, V represents the verification of both the attached certificate and the signature on the packet, and n represents the number of intermediate forwarders.

Table 2.1: Cryptographic Operations for Different Security Alternatives

Authentication Method	Source	Forwarder	Destination	Total operations
Hop-by-Hop	G	G+V	V	(n+1)*(G+V)
End-to-End	G	V	V	G+(n+1)V
Hybrid	2G	G+2V	2V	G+(n+1)*(2V+G)
Incremental	G	G+(n_{prev}+1)V	(n+1)V	(n+1)*(G+V) +$\sum_{k=0}^{n}$ kV

2.5 Identified Research Challenges

None of the previous works provides an efficient and comprehensive solution to secure PBR protocols in VANETs. Although the previous section has conducted distinguish studies on VANET's security, there are still several open problems including the following:

2.5.1 Security-Performance Tradeoff

Applying PKI with excessive use of digital signature, as in [4], introduces both more delay for the cryptographic operations and a larger packet size, which significantly affect the performance of the network. An efficient security scheme that introduces less security overhead is required. Therefore, deploying faster security tools and an appropriate signature scheme, if any, is preferred. Selecting a digital signature scheme includes tradeoff between signature generation and verification delay and the corresponding communication overheadwhich should be considered in designing a security scheme. As multi-hop routing

requires securing both end-to-end and hop-by-hop, security operations may be performed at each hop along the path, which make the tradeoff between security and efficiency very critical.

2.5.2 Suppressing Selfish Behavior

Multi-hop routing relies on the cooperative behaviour of forwarders. Selfish nodes may want to save their resources by not serving as relays for others. When a selfish node decides not to cooperate with others to deliver their packets but still uses them to send and receive its own messages, the network performance will be degraded. Therefore, routing protocol should consider trustworthy cooperative nodes in its forwarding strategy. Selfish and misbehaving nodes should also be excluded from the network. These routing services are major security research challenges and should be considered in designing an efficient security scheme.

2.5.3 Key Management

A comprehensive security scheme that uses public or symmetric key should provide a corresponding key management system. Key management includes generating, distributing, exchanging, updating, and revocating keys. It is considered a security research challenge in VANET with respect to some VANET's concerns such as scalability, interoperability, backward compatibility and forward secrecy.

2.6 Summary

VANET gained extensive interest in academia and industry due to the insistent demand of users including drivers, transportation systems designers, and car manufacturers. VANET

is one of the most promising technologies that enable VCS applications. These applications vary in purpose from safety applications to comfort applications. Applications include, but not limited to, warning messages such as accident warnings, congestion warnings, change lane warnings, and hazardous road status warnings, traffic management applications such as interactive traffic lights and adaptive traffic signs, or application related to passengers comfort such as file sharing and e-mail and internet access.

As many of these applications require multi-hop routing, routing protocol is key element in VANET system. PBR scheme is recommended for VANET as PBR protocols performs well in VANET's environment. In PBR, if a node wants to send a packet to another node, it first determines its location by location service, and then forward the packet toward that location. Forwarding process varies from protocol to another, but relies mainly on the information provided by neighbouring nodes.

Securing the process of PBR is a key research challenge in VANET. Applying PKI is a well-recognized solution to satisfy the primary security requirement for the end points. However, securing multi-hop routing includes both end-to-end and hop-by-hop security. Security schemes for PBR should consider security solution for one hop and multi-hop routing and resist PBR attacks. The design of such scheme should observe some security-efficiency tradeoff.

Only few work have addressed PBR security problem. Most comprehensive frameworks considered either end-to-end or hop-by-hop authentication which is not sufficient for multi-hop security. On the other hand, many studies focused on detecting falsified position information to improve PBR efficiency and detect some PBR attacks. The most notable work to secure PBR in VANET is given in[4] where the authors apply a hybrid signature scheme in PKI environment. This scheme provides the required level of security on the cost of communication and transmission overhead.

Chapter 3

ESPR: Efficient Security Scheme for Position-Based Routing in Vehicular Ad hoc Networks

ESPR is a novel security ware designed by the author with the goal of efficiently securing position-based routing (PBR) protocols efficiently. It employs cryptographic tools and a set of plausibility checks to meet the required security conditions and to enable vehicles to detect and avoid PBR attacks autonomously. In this chapter, the ESPR model is explained in detail: first, a preliminary section introduces some important concepts, followed by an overview of the model, then details of the ESPR functions, the corresponding key management scheme is then defined and the plausibility check set is described.

3.1 Preliminaries

This section describes the system model under consideration, and introduces basic security concepts, which are important in understanding the developed scheme.

3.1.1 System Model

As shown in Figure 3.1, the system under consideration consists of a Trusted Authority (TA) and a number of nodes. The TA is responsible for providing certificates and issuing secret and public keys to all legitimate nodes in the network. In addition, the TA is considered responsible to detect any compromised node, revoke its certificate and keep other nodes informed and up-to-date. It is assumed that the TA is owned and operated by a government or trusted institution, that does not threaten the users privacy and security. Moreover, the TA has sufficient computation and storage capabilities for the required tasks. The nodes in the system are either Roadside Units (RSUs) or On-Board Units (OBUs). RSUs are fixed units distributed throughout the entire network. They are connected to the TA and can communicate securely with it. OBUs are wireless devices embedded in vehicles in order to enable them communicate with one another or with RSUs. Both RSUs and OBUs are considered network nodes that have sufficient power, computation and storage resources, and they are enabled to obtain accurate and reliable position and time information.

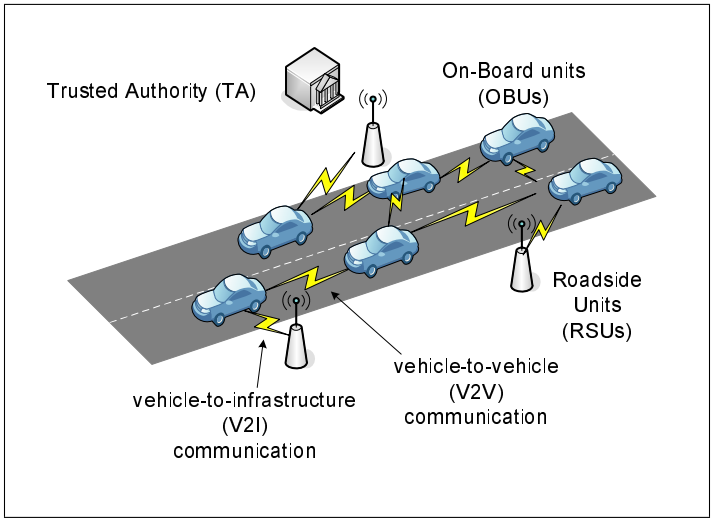


Figure 3.1: The System Model

The system model is primarily a public key infrastructure (PKI) system. The TA issues certificates and keys for legitimate network members in order to secure their communication. In case of a compromise, the TA distributes a revocation message to revoke the certificates and keys of the compromised node by the means of revocation lists. Legitimate nodes do not have sufficient incentives to disclose security materials, e.g., security keys, certificates, etc., to the revoked nodes.

The adversary model considers a variety of attackers with different goals and abilities. Attackers are willing to receive, modify, retransmit, inject, delete, or forge messages. Internal and external adversaries are considered; however, attackers with directional antennas and attacks launched below routing level (e.g., channel jamming at the physical layer) are not considered in this system.

ESPR supports unicast, geocast, and broadcast transmissions and their applications. It considers both one-hop applications, such as some warning messages, and multi-hop application, such as file transfer between non-neighbours. The details and the different approaches of the location service are not considered as it is orthogonal to the secure routing problem.

3.1.2 Elliptic Curve Digital Signature Algorithm

As the system model is a PKI system, it is important to select an appropriate Public-Key Cryptosystem (PKCS). Elliptic Curve Cryptosystem (ECC) is a PKCS that provides public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC has been deployed for Elliptic Curve Digital Signature Algorithm (ECDSA)[33]. ECC is recommended in VANET context [2] with respect to both signature size and processing time overhead. The details of elliptic curve algebra are beyond the purpose of this thesis.

The ECDSA has many advantages over other digital signature algorithms[2]. The bit size of ECDSA can be smaller with respect to the public-key, certificate, and signature

sizes. The length of the ECDSA public-key is about twice the security level. For instance, to achieve security level of 80 bits ECDSA requires a public-key with length of only 160 bits, whereas Digital Signature Algorithm (DSA) [34] requires 1024-bit public-keys to achieve the same security level. The signature size of ECDSA is $4t$ where t is the security level in bits. ECDSA takes T_{mul} to sign a message and 2 T_{mul} to verify it, where T_{mul} is the time required to perform a point multiplication on an elliptic curve [35]. ECDSA is adopted in the VANET IEEE 1609.2 standard as the employed signature scheme.

3.1.3 Hash Function and Hash Chains

A hash function is a mathematical function that converts large, variable-sized data into a small, fix-sized hash value. A hash function has the following properties:

- Forms a unique image of the message; it should not be possible to deterministically find another message that creates the same hash value
- Designed in such a way that as small a change as one bit in the message will produce unpredictable changes of the hash value bits; i.e., every bit of the hash value changes with a probability of 0.5
- Can be applied to any size of message and produce a fixed size hash value
- Easy and efficient to compute but is computationally infeasible to invert

Hash function allows for the detection of message modification. Keyed hash function is used to provide both data integrity and message authenticity. Thus, it called Hash-based Message Authentication Code (HMAC). Secure Hash Algorithm (SHA) is designed to implement hash function. SHA-1 [36] produces 160-bit hash value and supports a cryptographic strength of 80 bits. The key of HMAC can be of any size as it can be hashed to produce a key compatible with the length of the algorithms block size.

A hash chain is a successive application of a hash function (h) to a value v to produce a chain of irreversible values $\{v_0, v_1, \cdots, v_j\}$, where $v_0 = v, v_i = h(v_{i-1})\ \forall\ 1 \leq i \leq j$, as shown in Figure 3.2.

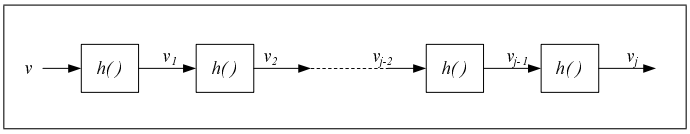


Figure 3.2: Hash Chain

3.2 ESPR: An Overview

ESPR uses both cryptographic primitives and logical checks to secure the process of PBR. It uses digital signature on the mutable fields to achieve End-to-End authentication, non-repudiation, and data integrity. Moreover, it uses HMAC on the mutable fields to secure Hop-by-Hop communication, where legitimate users always share a common key. ESPR proposes a corresponding key management scheme for key initialization, revocation, and updating processes. Logical checks, or plausibility checks, are proposed to increase the scheme's robustness.

3.2.1 System Initialization

At the initialization phase, the required security materials are prepared by the TA and securely loaded into each node. New nodes can join the network any time by loading these security materials into their systems. Network members may need to periodically reload their security materials. Under the PKI system environment, the TA should prepare the following:

- A set of private-public key pairs to be used by the nodes to sign their messages.

- A set of certificates. Each key pair is associated with a corresponding certificate signed by the TA. The certificate includes the public key, user identity, and a predetermined validity period.
- A set of secret keys, which are used to manage the HMAC shared key. This set will be referred as the secret key pool KP. KP has l different keys, *i.e.*, $KP = \{k_i | 1 \leq i \leq l\}$
- Secret key (k_g), which is used as a shared secret key between legitimate nodes.
- Selection of a hash function h.
- A set of hash chain values $V = \{v_i | 0 \leq i \leq j\}$, where j is large enough to accommodate the number of revocation processes that occur during the life-time of the network.

Before each node joins the network, it should be loaded with the following:

- A set of private-public key pairs and corresponding certificates with predetermined validity periods. This set is used to achieve End-to-End authentication, data integrity, non-repudiation, anonymity, and traceability by the TA.
- A set of secret keys R_u consisting of m keys randomly selected from the key pool KP. This set helps the key management operations for the shared secret key K_g.
- k_g.
- h.

3.2.2 Beaconing

Beaconing messages are periodical one-hop broadcast messages that include nodes identities and locations to enable PBR functions. In ESPR, nodes update their location tables only

based on the receive beacons, where each node insets its information, appends its certificate and a timestamp (time of packet generation), signs the entire message using its private key corresponding to the attached certificate, and attaches this signature. When a node receives a beacon, it cryptographically verifies the source's signature and certificate. It also applies some plausibility checks on the information carried by the beacon, e.g., time and location. Hence, routing tables have plausible information provided by legitimate neighbours, which helps to take better routing decisions and to avoid routing attacks. One-hop messages, other than beacons, follow the same principles.

3.2.3 Destination Location

Location service is one of the main PBR services. In location service, a node sends a multi-hop query message to obtain the destination location. In literature, different approaches have been proposed for location service, e.g., using trusted location servers. The sender waits until receiving a location response. Both location queries and location responses are multi-hop messages. Therefore, securing multi-hop transmission secures the location service. However, ESPR does not discuss the details and the different approaches of location service as it is considered independent to the secure routing problem. In ESPR analysis and evaluation, it will be assumed that the destination location is known.

3.2.4 Multi-hop Forwarding

Many unicast and geocast VANETs applications require multi-hop forwarding to deliver messages to their destinations. In ESPR, the source of a message signs the payload and the immutable fields in the header after attaching its certificate and a timestamp. This provides authentication and non-repudiation to the end nodes and maintains the data integrity for the carried information. The source and each intermediate forwarder selects

the next hop, from the registered neighbours in its routing table, based on the routing strategy of the routing protocol.

The mutable fields are not protected by the source's signature as they are modifiable at each intermediate hop. Each forwarder updates these fields and computes a message authentication code (MAC) on both the mutable fields and the source's signature using k_g. This achieves authentication between intermediate nodes and guarantees mutable fields integrity. Upon receiving a packet, a recipient verifies the MAC and the source's signature and certificate. The property of fast verification of MAC helps to improve the network performance and avoid some routing attacks as will be discussed later. Figure 3.3 shows the general structure of the ESPR packet.

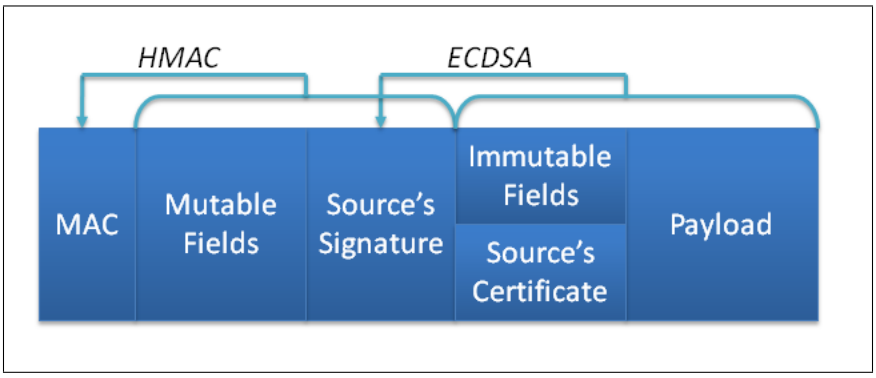


Figure 3.3: General Structure of the ESPR Packet

3.3 ESPR: Function Model

ESPR can be described in terms of its major functions. In this section, a deeper view and more details of ESPR are provided: the security fields added by ESPR are discussed and a corresponding message format is suggested, the proposed approaches to secure outgoing messages and verify incoming messages are presented, and the proposed revocation mechanism is introduced.

3.3.1 Message Format

The general format of ESPR packet was introduced in Figure 3.3. With respect to selecting an 80-bits security level, the size of ECDSA public key and the corresponding signature are 160 bits ($20B$) and 320 bits ($40B$) respectively. The certificate includes the node identity (or pseudonym), its public key, validity period, and the TA's identity and signature. A certificate size of $125B$ is considered.

The content of MAC field is the result of HMAC function with inputs of mutable field contents and the source's signature. The size of this field is 160 bits ($20B$) with respect to the security level and the hash algorithm (SHA-1).

The mutable fields are related to the routing protocol. It includes some control fields, such as the routing mode field in GPSR, and other routing information such as last sender information and number of hops. The immutable fields are the fields in the original packet header that include unmodifiable information such as the source and the destination nodes. Payload data and source's signature and certificate are immutable.

The size of the payload field varies and depends mainly on the corresponding application. For example, it is recommended for safety messages to have a small size, e.g. $100B$. An ESPR packet is illustrated in Figure 3.4.

3.3.2 Securing Outgoing Messages

Algorithm 1 Shows the ESPR procedure that secures outgoing messages including beacons, originated one-hop or multi-hp messages, and received messages that have to be forwarded. It describes the general process from a security point of view and can be easily applied to any specific PBR protocol.

In ESPR, only legitimate nodes are allowed to participate in the network services. Each member shoud have a valid certificate in order to generate a message, and k_g in order

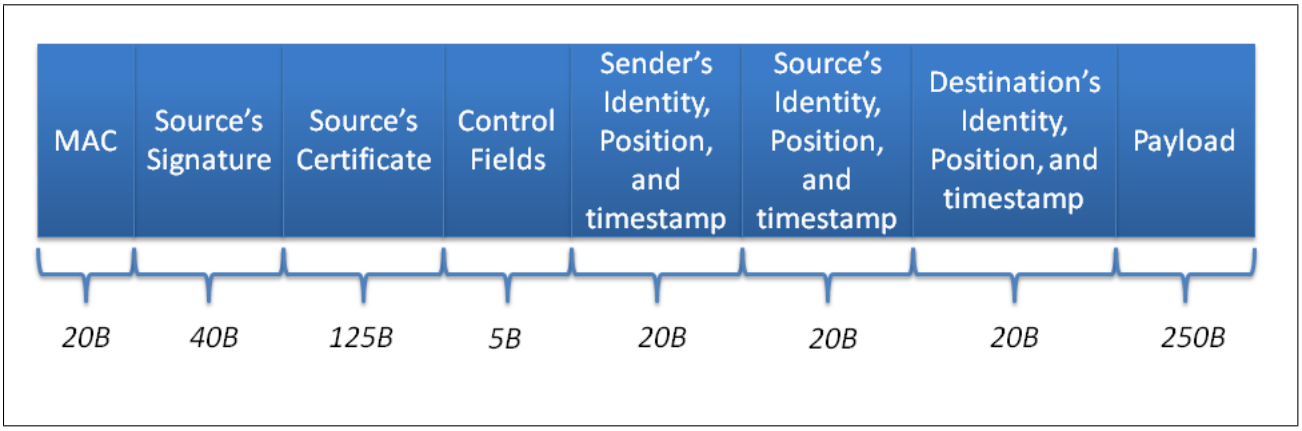


Figure 3.4: ESPR Message Format

to forward a message. Network members embers sign messages that they originate and append their signatures and certificates. However, they do not need to sign messages that they receive for routing purposes. Instead, they only calculate and append HMAC using k_g as shown in steps (24-30) of Algorithm 1.

3.3.3 Incoming Messages Verification

ESPR applies two types of verification on a received message: cryptographic verification and plausibility checks. The cryptographic verification processes verify nodes legitimacy and data integrity, via the described cryptography tools, while the plausibility checks verify the content of the message to make sure that it carries plausible information. The complete set of plausibility checks are presented in section 3.5.

Received messages are either beacons, one-hop unicast messages targeting the recipient, broadcast or geocast messages, or multi-hop unicasted messages. In ESPR, any received message should be cryptographically verified. A recipient of a message verifies its sources certificate and signature; it also verifies its HMAC in the case of multi-hop messages. Certificate verification requires the availability of the TA's public-key. Signature verification requires the source's public-key, which is included in its certificate. Finally, HMAC

verification requires the availability of k_g.

Algorithm 2 shows the verification procedure to verify a received message. The algorithm is designed properly to increase the efficiency of ESPR as logical checks are usually faster than the cryptographic operations and the symmetric-key cryptography verification is much faster than the verification of public-key cryptography.

Algorithm 1 Message Transmit/Forward

Require: Valid certificate and/or K_g

if the message is one-hop communication **then**
    Inset the vehicle's information in source and sender routing header's fields
    Reset the overhearing timer for this message, T_{Oi}=0
    if the message is a beacon **then**
        Set the control and destination fields to indicate a one-hop broadcast message
        Insert the information required by the routing protocol (if any)
        Insert the last known revocation process version *ver*
    else
        Insert the destination-location information extracted from the routing table into the destination field
    end if
    Select a valid certificate and its corresponding private key
    Append the certificate and a timestamp to the message
    Sign the entire message using the private key
    Append the signature to the message
else ▷ i.e., multi-hop message
    if the vehicle is the source of the message **then**
        Get the destination's location via location service
        Inset the source and destination information in the immutable routing header fields
        Select a valid certificate and its corresponding private key
        Append the source's certificate and a timestamp
        Sign the entire message except for the mutable fields using the private key
        Append the signature to the message
    end if
    Insert the information of the next forwarder and a timestamp in the mutable sender field in the routing header
    Modify the mutable fields according to the routing protocol (if required)
    Calculate HMAC on the mutable fields and the signature field using the shared secret key K_g
    Append the HMAC to the message
    Set the overhearing timer for this message T_{Oi}
end if
Send the message
Run the Overhearing procedure for T_{Oi}

Algorithm 2 Receiving a Message

Require: TA's Public-Key and K_g (in certain cases)

```
1: Perform the plausibility checks as indicated in section 3.5
2: if the message does not pass the plausibility checks then
3:     Drop the message
4: else
5:     if the vehicle is the destination of the message then
6:         Verify the source's certificate using the TA's public key
7:         if invalid then
8:             drop the message
9:         else
10:            Verify the source's signature using the source's public key
11:            if invalid then
12:                drop the message
13:            else
14:                process the message
15:            end if
16:        end if
17:    else                                   ▷ i.e., the vehicle is a forwarder
18:        Calculate HMAC on the mutable fields and the source's signature using K_g
19:        Compare it with the HMAC appended to the received message
20:        if a mismatch occurs then
21:            drop the message
22:        else
23:            Verify the source's certificate using the TA's public key
24:            if invalid then
25:                drop the message
26:            else
27:                Verify the source's signature using the source's public key
28:                if invalid then
29:                    drop the message
30:                else
31:                    execute Algorithm 1
32:                end if
33:            end if
34:        end if
35:    end if
36: end if
```

3.3.4 Trust Revocation

When a compromised node is found, or a node is decided to be revoked, the TA identifies its identity and excludes it from the system. This is usually achieved by the means of Revocation Lists (RL), where the TA broadcasts the identities or the certificates of the revoked nodes. Each node in the system maintains a list of the revoked nodes to avoid any communication with them. RL management still has many open issues and challenges to be resolved. Rrecent revocation-related studies can be adapted to complement the ESPR scheme, e.g.,[37], [38], and [35].

In ESPR, the revocation process is triggered by the TA. Legitimate nodes report routing misbehaviour and suspicious cases to the TA. Each message includes its originators signature and certificate so the TA is able to trace and extract the identity of the source node. For example, when a node receives a message from a legitimate network member with falsified information, or when it detects routing attack behaviour, it reports the suspicious message with any other required information to the TA. Based on some criteria, the TA takes a revocation decision and broadcasts a revocation message.

When a legitimate node u is to be revoked, its certificates, secret keys set R_u, and K_g must be revoked. The revocation message includes sufficient data to revoke the certificates of u, update the common secret keys hold by the unrevoked nodes (if any), and securely distribute a new shared secret key k_g. The details and the corresponding algorithms of keys renewal will be shown in section 3.4.

ESPR follows a probabilistic key distribution scheme to manage k'_g. When a member is to be revoked, the TA searches for M, the identity of the non-compromised secret key k_M that is shared by the majority of the unrevoked members. With the help of v_{j-ver}, the TA calculates the new secret key k'_g, where v_j is the value in the hash chain as shown in Figure 3.2 , and *ver* represents the revocation version. To enable the unrevoked nodes to update their keys and calculate the new secret key, the ESPR revocation pattern is defined

as follow:

$$Kmsg = (ver||M||IDrev_{key}||enc_{k_M}(v_{j-ver})) \tag{3.1}$$

where $IDrev_{key}$ is a list of the identities of the revoked keys, and $enc_{k_M}(v_{j-ver})$ is the symmetric encryption of v_{j-ver} using the key k_M. Therefore, the final revocation message will be:

$$REV_{msg} = (CRL||Kmsg||Sig_{TA}) \tag{3.2}$$

where CRL is a list of the certificates of the revoked nodes, and Sig_{TA} is the TA signature on $CRL||Kmsg$.

3.4 ESPR: Key Management

The cryptographic operations in ESPR depend on two types of keys, symmetric and asymmetric keys. The deployment of ESPR is mainly associated with designing an efficient corresponding key management scheme to distribute, revoke, and update these keys. The ESPR key management scheme is based on the traditional PKI system, where the TA issues certificates and public-private key pairs to the network members, and broadcasts revocation messages to revoke the trust of any of them. However, ESPR justifies this process and combines it with the management of the symmetric key k_g. The management scheme can be described via its major functions: system setup, member registration, member tracing, membership revocation and keys update.

3.4.1 System Setup

The TA should prepare some security material before initializing the system. First, it defines the elliptic curve domain parameters, generates public-private key pairs, and selects the hash function h. Then, the TA selects an initial key k_g and a key pool $KP = \{k_i | 1 \leq i \leq l\}$ where $k_i \in \mathbb{Z}_q^*$, q is a prime number and l is a large number indicating the pool size. The TA should also select a key pair for itself in order to sign members' certificates. Finally, the TA selects a secret value v and applies the hash function h j times on v to produce a set V of hash chain values, where j is large enough to accommodate with the number of revocation processes occuring during the life-time of the network. Algorithm 3 describes this setup phase.

3.4.2 Member Registration

To initiate the system, each member u (RSU or ORU) should register in the system and obtain its required security materials from the TA. In this phase, the TA provides each legitimate node with a number of certificates, k_g, and a set of secret keys R_u that are randomly chosen from the key pool KP.

For privacy purposes, the TA issues each node with a number of predetermined validity period certificates. Each certificate includes the node's pseudonym, a public-key $Q_u i$, a validity period, and the TA's signature. The TA signs each certificate using its private key d_T.

Based on the probabilistic key distribution in [39], the TA randomly assigns m secret keys from KP to each member; thus, members share some keys. The sets of secret keys are used to manage k_g as will be shown later.

Algorithm 3 System Setup

Require: EC Domain Parameters, Random Number Generator

Select random number d_T
Set the TA private key d_T
Select the corresponding public key Q_T ▷ According to the EC domain parameters
for $i \leftarrow 1, N$ **do** ▷ N is the number of the certificates required by the system
    Select a random number d_i as a private key
    Select the corresponding public key Q_i ▷ According to the EC domain parameters
end for
for $i \leftarrow 1, l$ **do**
    Select a random number $k_i \in \mathbb{Z}_q^*$, where q is a prime number
end for
Set the TA key pool $KP = \{k_i | 1 \leq i \leq l\}$
Select an initial secret key K_g ▷ to be shared between all the unrevoked OBUs
Choose hash functions $h : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
Select a secret value $v \in \mathbb{Z}_q^*$ and set $v_\circ = v$
for $i \leftarrow 1, j$ **do** ▷ to obtain a set V of hash chain values
    Set $v_i = h(v_{i-1})$
end for
Set $V = \{v_i | 1 \leq i \leq j\}$

Algorithm 4 Member Registration

for all OBU_u in the network, TA **do**
    for $i \leftarrow 1, M$ **do** ▷ M is the number of certificates allocated to each node u
        Upload a key pair (d_i,Q_i)
        Prepare and sign certificate i
        Upload the certificate i
    end for
    for $i \leftarrow 1, m$ **do** ▷ m is the number of secret keys allocated to each node u
        Select a random number $a \in [1, l]$
        Upload the secret key $k_a \in KP$ in OBU_u
    end for
    Upload the shared secret key k_g
    Upload the secret hash chain value v_j
    Announce the hash function h
end for
Announce the TA's public key Q_T to all the OBUs

In addition to uploading certificates and a secret keys set to each member, the TA securely uploads k_g, the hash chain value v_i, the TA's public key Q_T, and announces h. Algorithm 4describes the member registration process. The procedure to follow when a new member is joining the network during its operation is similar.

3.4.3 Member Tracing

The author considers anonymity to preserve users privacy; therfore, member tracing is a necessity to resolve any dispute. In ESPR, any member originates a message attaches its certificate and signs the message. The TA maintains a table that binds the real identities to the corresponding pseudonyms. Thus, when a network member detects misbehaviour or an authentic message containing falsified information, it simply reports the message to the TA. The TA then traces the attached pseudonym to the certificate and identifies the message originator.

3.4.4 Membership Revocation and Keys Updating

The revocation process is triggered by the TA when there is an OBU_u to be revoked. The certificates of OBU_u must be revoked. In addition, the secret key set R_u of OBU_u and K_g are considered revoked; hence, a new secret key $K_g^{\setminus}$ should be securely distributed to all the unrevoked OBUs. Each unrevoked OBU should securely update the compromised keys in its key sets R [39] [35]. The revocation and updating process can be described in the following steps:

1. The TA searches its database to determine the identity (M) of the non-compromised secret key k_M that is shared by the majority of the unrevoked OBUs. The TA then selects the value v_{j-ver} of the hash chain values, where v_j is the last value in the

hash chain as shown in Fig. 3.2, and ver is an integer indicating the revocation version, i.e., the number of the revocation processes performed since the network initialization. After that the TA calculates the new secret key:

$$K_g^{\setminus} = h(K_g, v_{j-ver}) \tag{3.3}$$

Then, the TA prepares the following key update message,

$$Kmsg = (ver||M||IDrev_{key}||enc_{k_M}(v_{j-ver}))$$

where $IDrev_{key}$ is a list of the identities of the revoked keys, and $enc_{k_M}(v_{j-ver})$ is the symmetric encryption of v_{j-ver} using the key k_M. Finally, the TA broadcasts the following message:

$$REV_{msg} = (CRL||Kmsg||Sig_{TA})$$

where CRL is a list of the certificates of the revoked OBUs, and Sig_{TA} is the TA signature on $CRL||Kmsg$.

2. After receiving REV_{msg}, each OBU_y executes Algorithm 5 to extract the new shared secret key and update the secret key set if necessary.

3. OBU_y has to execute Algorithm 6 to get v_{j-ver} and $K_g^{\setminus}$. If OBU_y has K_M, it can independently get v_{j-ver} and calculate $K_g^{\setminus}$ according to step (3). Otherwise, OBU_y gets v_{j-ver} and $K_g^{\setminus}$ from its neighboring OBUs as indicated in steps 5-13.

4. OBU_y has to execute Algorithm 7 to update its key sets R_y. In step 11, $ver_{|_{missed}}$ and $IDrev_{key|_{missed}}$ denote the revocation version and the list of identities of the revoked keys of a missed revocation process, respectively.

Algorithm 5 Processing Revocation Messages

Require: $REV_{msg} = (CRL||Kmsg||Sig_{TA})$

1: Verify Sig_{TA} using the public key of the TA, Q_T
2: **if** invalid **then** Exit
3: **else**
4: Run Algorithm 6 to get v_{j-ver} and $K_g^{\setminus}$
5: Run Algorithm 7 to update the key set of OBU_y
6: **end if**
7: Store ver and $IDrev_{key}$
8: Erase K_g, the hash chain values, and the original compromised secret keys.

It should be noted that ESPR enables an OBU to update its compromised keys even if it missed revocation processes, provided that it will pick one revocation process in the future. This is very convenient in the vehicular environment.

3.5 ESPR: Plausibility and Monitoring Checks

Plausibility checks are a set of logical tests and corresponding procedures to ensure that the received message follows some logical rules, and the sent messages are more likely to be delivered. The checks include tests for information plausibility in order to avoid and detect routing attacks, and procedures in case there is a suspicion of a routing attack. Together with the

Algorithm 6 Obtaining v_{j-ver} and $K_g^{\setminus}$

if k_M exists in R_y **then**
  Decrypt $enc_{k_M}(v_{j-ver})$ using k_M to get v_{j-ver}
  Set the new secret key $K_g^{\setminus} = h(K_g, v_{j-ver})$
else
  Broadcast a request and $cert_{OBU_y}(ID_y, Q_y)$ to get v_{j-ver} and $K_g^{\setminus}$ from neighboring OBUs
  Start a timer T_1
  Any neighboring OBU of OBU_y having v_{j-ver} uses the public key (Q_y) of OBU_y, included in its certificate, to encrypt $v_{j-ver}||K_g^{\setminus}$ and sends them to OBU_y
  if the encrypted v_{j-ver} is received **then**
    Decrypt $v_{j-ver}||K_g^{\setminus}$ using the secret key d_y corresponding to Q_y to get v_{j-ver} and $K_g^{\setminus}$
  else
    if T_1 is timed out **then** Go to 5
    end if
  end if
end if

Algorithm 7 Updating the Key Set of OBU_y

Require: $K_g^{\setminus}$ and v_{j-ver}
if not previously missing any revocation message **then**
  if possesses compromised secret keys $\{k_i\}$ in $IDrev_{key}$ **then**
    Update the secret key k_i as $k_i^{\setminus} = h(k_i, v_{j-ver})$
  else Exit
  end if
else Set $n = ver$
  while $n \neq v_{ver_{last}}$ **do** ▷ ver_{last} is the last received revocation version
    Set $v_{j-n+1} = h(v_{j-n})$
    Set $n = ver + 1$
  end while ▷ this loop outputs $\{v_{j-ver+1}, v_{j-ver+2}, \cdots, v_{ver_{last}-1}\}$
  Broadcast a request to the neighboring OBUs requesting $ver_{|missed}$ and $IDrev_{key|missed}$ for all the missed revocation processes
  for each received value of $ver_{|missed}$ **do**
    Find the value of $v_{j-ver_{|missed}}$ from $\{v_{j-ver+1}, v_{j-ver+2}, \cdots, v_{ver_{last}-1}\}$
    for each possessed key $k_i \in IDrev_{key|missed}$ **do**
      Update the secret key k_i as $k_i^{\setminus} = h(k_i, v_{j-ver})$
    end for
  end for
end if

proposed cryptographic scheme, the set of plausibility checks support routing protocols to avoid and detect routing attacks, and to perform well even in the presence of such attacks.

3.5.1 Spatial Checks

Spatial checks are a set of tests to be run on the received messages. In PBR, it is important to provide correct and accurate position information in order to achieve efficient message routing. ESPR requires each node to sign its beacons, which include its location information. Thus, each node is responsible for providing correct position information. The set of the proposed spatial checks are:

- Communication range: each recipient of a message must ensure that it falls within the sender's communication range. The distance between the sender and the recipient at the message generating time should be plausible. Each recipient checks that:

$$d_r - d_s \leq C_r + \epsilon \tag{3.4}$$

  where d_r and d_s are the locations of the receiver and the sender, respectively at the message generating time found in the timestamp field, C_r is the nominal communication range of the node in the system, and ϵ is the maximum possible error. Errors include inaccuracy of a positioning system.

- Speed and density checks: In this check, the recipient ensures that the received information follows the Greenshield's speed-density relation[40]. In the Greenshield model, the maximum plausible speeds for vehicles are limited by the vehicles' density with respect to the following relation:

$$v(k) = v_f - \frac{v_f}{k_j}k \tag{3.5}$$

where v_f is the free-flow speed (i.e., the maximum speed), k_j is the jam density (i.e., the maximum plausible density in the communication range), and k is the current density.

The relation is adopted to check that the speed of the transmitting vehicle and the density of the neighboring vehicles are plausible as follows: when a vehicle receives a message, it calculates the number of its neighboring vehicles from its routing table; then it uses eq.3.5 to calculate the plausible average speed of its neighboring vehicles as a function of the neighboring vehicles' density. After that, it ensures that:

$$v_s \leq v(k) \pm \triangle \tag{3.6}$$

where v_s is the speed of the sender, and $\triangle$ is a speed margin factor to accommodate for the speed variations.

- Moved distance: The receiver of a message can check the plausibility of the moved distance by the transmitter with respect to the last known position of the transmitter by ensuring that:

$$l_{s2} - l_{s1} \leq (t_{s1} - t_{s2}).v(k) \tag{3.7}$$

where l_{s2} is the location of the sender included in the received message, t_{s2} is the timestamp included in the received message, and l_{s1} is the location of the sender at time t_{t1} in the routing table.

- Map location: Assuming that each vehicle is equipped with a GPS receiver, the recipient of a message must ensure that the location of the sender is not in an improbable location (house, river, etc).

3.5.2 Temporal Check

Each beacon and data packet includes a timestamp of the sending time t_s. Upon receiving a packet, each node checks that it has received the packet in reasonable time with respect to the maximum plausible time for processing and transmitting such packets:

$$\triangle_{t-min} \leq t_r - t_s \leq \triangle_{t-max} \tag{3.8}$$

where t_r is the receiving time, $\triangle_{t-max}$ is the maximum plausible time for one-hop packet transmission and processing, and $\triangle_{t-min}$ is the minimum delay for packet transmission and processing. Thus, replayed messages after a certain time, and messages with timestamps belonging to the future are detectable.

3.5.3 Strategy Check

In PBR, different protocols have different forwarding strategies. When a vehicle receives a packet to be forwarded, it should check that it falls within a feasible forwarding region with respect to the node's position, the sender's position, the destination's position, and any other information from the routing protocol. For example, Figure 3.5 illustrates the feasible senders position region in which they can send a packet to recipient R in order to deliver the packet to its destination D using the greedy routing strategy.

3.5.4 Overhearing

When a node sends a packet to be forwarded, it sets a timer and expects to hear the packet being forwarded. If the packet is not transmitted, it re-transmits it to the next node in the routing table, according to the forwarding strategy, and avoids sending any packet to the suspicious node for N seconds. Packets can not be overheard for many reasons,

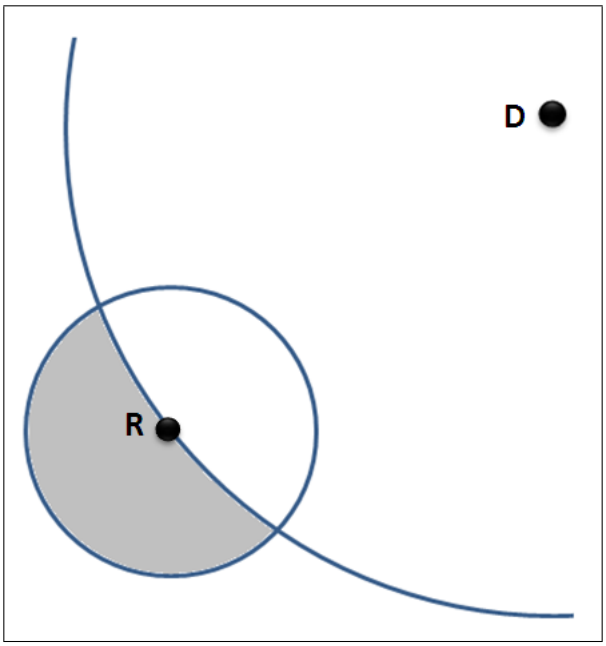


Figure 3.5: Example of Sender's Feasible Region in Gready Routing

e.g., collisions, link breakage; hence, nodes only retransmit the packets that have not been heard, and do not immediately report the suspicious nodes to the TA.

3.5.5 Content Checks

Checking message contents in terms of duplicated or expired content will effectively preserve the network resources. In addition, monitoring the contents in terms of message generating rates helps to preserve bandwidth; for example, sending beacons or location inquires at a high rate should be ignored and reported. This check will be significantly effective if packet generating rates are defined with respect to the node's type and application.

3.6 Summary

In this chapter, ESPR was proposed to provide a security solution for PBR protocols. ESPR consists of two major parts: cryptographic scheme and plausibility checks. The cryptographic scheme deploys both symmetric and asymmetric keys, and provides a corresponding key distribution system. ESPR supports PBR protocols with both primary security requirements, and robustness against defined routing attacks.

ESPR deploys the PKI system with an elliptic curve digital signature, and HMAC function with a shared secret key between legitimate nodes, in order to secure multi-hop communication. Every legitimate node should have a valid certificate with a corresponding private key and an up-to-date shared secret key. Any node generates a message, including beacons, signs the immutable fields of the message, using its private key, and attaches the corresponding certificate. Forwarders cryptographically verify both the signature and the HMAC value on the mutable fields, update these fields, and calculate a new HMAC value, that replaces the previous one.

In case of revocation, the TA broadcasts a revocation message containing sufficient information to revoke the trust of the targeted node, and update the keys with the legitimate nodes securely. Revoking the certificates is done through revocation lists. Managing the shared key is done by a probabilistic key distribution scheme. The proposed key distribution scheme is flexible with the vehicular environment; i.e., vehicles are able to update their keys even if they have missed a number of revocation processes.

Plausibility and monitoring checks are proposed to complement the cryptographic scheme and enable ESPR to avoid, detect, and recover from different routing attacks. ESPR check set includes spatial checks, temporal checks, strategy checks, content checks and overhearing procedure. These checks are run autonomously by nodes and any detected misbehaviour is reported to the TA.

In conclusion, ESPR is a comprehensive security scheme to secure the different processes of position-based routing in the context of vehicular networks. It supports one-hop and multi-hop applications, and unicast, Geocast, and broadcast transmissions. Using symmetric and public key cryptography in addition to some logical checks, ESPR is capable of avoiding, detecting and recovering from many routing attacks.

Chapter 4

ESPR: Analysis and Performance Evaluation

In this chapter, the proposed security scheme is evaluated analytically and through extensive simulations. A security analysis is provided with respect to a variety of network layer attacks. In addition, the efficiency of ESPR is analyzed in terms of both bit-cost and cryptography delay. Finally, simulation results are conducted to evaluate the system under different scenarios and attacks.

4.1 Security Analysis

Digital signature on the generated messages guarantees authentication, data integrity, and non-repudiation. Thus, an external attacker cannot poison routing tables by forged beacons, impersonate identities of authorized members, or modify or inject packets in an unauthorized manner. Therefore, the delivered information from a legitimate source should be trustworthy. Moreover, any detected misbehavior of a legitimate member is traceable and causes trust revocation.

Because attackers can replay authentic beacons or packets to forge legitimateness, a combination of plausibility checks (spatial, temporal and content) verifies message freshness and prevents message duplication. Therefore, replay attacks, including replay-based impersonation attack, are impossible.

Spatial checks effectively tighten the plausible geographical area of the claimed falsified position and eliminate all implausible location claims. By spatial checks, the plausible locations are reduced to some positions within the transmission range of a receiver and restricted by the roadways of this area (in the case of vehicles). In other words, spatial checks limit the options available, forcing a smart attacker to claim a position within a very narrow area to fool a vehicle. However, this claim can be easily detected by other nodes in the attackers transmission range. Thus, spatial checks are capable of detecting attacks that depend on announcing falsified-positions, and wormhole attacks. The probability of detecting beacons with falsified-position information is higher in dense networks.

In Sybil attacks, the attacker uses many identities simultaneously. In the case of using predetermined validity periods in the certificates, cryptographic validation is sufficient to detect this attack. If replaying identities is used, spatial, temporal and content checks can overcome this attack, as mentioned. In the case of using valid and real certificates, spatial checks by some nodes in the attacker's transmission range can detect and report its misbehavior and identity.

The sinkhole attack includes both the announcement of a falsified-position and selfish behavior of packet dropping. The detection of the claimed position follows the same detection methods previously described. Moreover, the overhearing check and its corresponding procedure are designed for the packet dropping part. However, the sinkhole attack is still valid if the node density is very low and nodes are isolated by the network's nature.

A routing loop can occur naturally, for a limited period of time, or intentionally by an attacker. In the intentional routing loop attack, an attacker can either ignore the routing

strategy and pass the packet back to one of the previous nodes, or forge a position to first get the packet and then forward it in order to form a loop. The misbehavior of the routing decision is detectable by the strategy check at the recipient node. The falsified position can be detected by spatial checks with respect to the node density. Content check prevents endless loops and saves bandwidth.

Routing packets among legitimate members prevents external attacker from launching routing attacks. As authentication is required to modify routing tables, packets are not forwarded to unauthorized nodes for routing purposes. Moreover, received packets are checked first to ensure that they have been transmitted by legitimate members. Thus, the majority of attacks are avoided by the proposed cryptographic scheme, and the rest of them, mostly performed by internal attackers, are handled by the proposed plausibility checks. ESPR includes reporting detected and suspected identities to the authority, which revokes trust from internal attackers, thereby turning them into external attackers.

Another advantage of ESPR is forward secrecy. Since the values of the hash chain, included in the revocation messages, are released to unrevoked nodes starting from the last value of the hash chain, and given the fact that a hash function is irreversible, a revoked node cannot use a hash chain value $v_{j-ver+1}$ received in a previous revocation process to get the current hash chain value v_{j-ver} . Consequently, a revoked node cannot update its key set. In addition, a revoked node cannot get v_{j-ver}, which is necessary to update its key set, or $K_g^{\setminus}$ from the neighboring nodes, since the revoked nodes' certificates are in the updated CRL, which prevents unrevoked nodes from forwarding $v_{j-ver}||K_g^{\setminus}$ to the revoked nodes. Accordingly, ESPR guarantees forward secrecy.

4.2 Efficiency Analysis

In addition to securing VANETs communication, ESPR improves its efficiency. Due to the highly dynamic nature of the VANET local topologies, a faster security scheme means a smaller los- rate and less end-to-end delay. By decreasing the cryptography delay required by each forwarder to verify both the originator's signature and the sender's signature in the hybrid scheme [4], multi-hop routing performs better. ESPR requires each forwarder to perform a symmetric key-based verification of the mutable fields first, only then the originator's signature is verified, which efficiently reduces the processing time for each intermediate hop. Therefore, it is less likely that the messages destination will change its location, or that the link with a neighbor will be broken.

Fast message verification protects members from some resource depletion attacks. Many attacks exploit the verification stage of the security module and jam the network. For example, sending forged packets at a high rate exhausts recipients' resources in verification processes, especially for systems with signature-based verification. Using the fast HMAC verification significantly reduces the verification time that is required to detect dummy packets injected by external attackers and decreases the effects of such attacks.

Packets are routed among legitimate nodes only. Members who succeed to present valid certificates can use the network services and participate in the routing process. Therefore, packets are more likely to be delivered. On the other hand, legitimate members who have not updated their shared secret key k_g cannot contribute in routing efficiently. In fact, this happens with a very small probability. Since a member is connected to some other nodes, its keys are easily updated. Moreover, unauthorized ad-hoc nodes that can participate in routing and improving the network performance are not allowed to participate for security purposes.

Plausibility and monitoring checks in the ESPR system assist the network to achieve

better performance. By curtailing routing attacks, and by dropping forged, duplicated and expired packets, ESPR conserves the network's bandwidth for other valid packets. Furthermore, the overhearing procedure helps to recover packets, in packet dropping attacks, and increases the overall delivery rate.

4.2.1 Communication Overhead

The multi-hop communications overhead incurred due to securing the routing process is a major evaluation metric for security schemes. In the hybrid scheme [4], the communications overhead in each packet consists of a source node certificate, signature of the source node, certificate of a forwarder, and signature of the forwarder on the mutable fields. In the ESPR scheme, the communications overhead in each packet consists of a source node certificate, signature of the source node, and an HMAC calculated by a forwarder on the routing header. It should be noted that in the ESPR scheme there is no need to insert any certificates for the intermediate node as the next-hop needs only the shared key K_g to verify HMAC. Elliptic Curve Digital Signature Algorithm (ECDSA) [33] is considered where signature consists of two elliptic curve points. ECDSA implemented on an MNT curve [41] is considered where an elliptic curve point is represented by 160 bits. Moreover, a certificate in IEEE1609.2 standard is 125 bytes. Moreover, Secure Hash Algorithm 1 (SHA-1) [36] is considered as the employed HMAC function, where the size of the output hash is 160 bits. Consequently, the communications overhead incurred due to securing the routing process in the hybrid scheme and ESPR is 330 bytes and 185 bytes, respectively. Accordingly, the ESPR scheme decreases the incurred communications overhead by 43.9% compared to the hybrid scheme.

4.2.2 Cryptography Delay

The cryptography delay T_{crypt}, which is defined as the incurred delay due to the performed cryptography operations for securing the routing process, is another key metric to evaluate security systems. Let T_{mul} and T_{hash} represent the time required to perform one point multiplication on an elliptic curve and HMAC, respectively. In ECDSA, a certificate verification, signature generation, and signature verification takes $2T_{mul}$, T_{mul}, and $2T_{mul}$, respectively. In the hybrid scheme, the source has to generate two signatures, on the mutable fields and on the immutable fields, which takes $2T_{mul}$. Moreover, each subsequent node along the route has to verify the certificates and the signatures of both the source and the previous forwarder, which takes $8T_{mul}$ in total. In addition, each intermediate node needs T_{mul} to sign the mutable fields after updating it. Consequently, T_{crypt} for the hybrid scheme is $(10 + 9n)T_{mul}$, where n is the number of intermediate nodes.

In the ESPR scheme, the source has to sign the message, which requires T_{mul}, and calculate HMAC on the routing header, which requires T_{hash}. In addition, each subsequent node in the route has to verify the certificate and the signature of the source node, verify the received HMAC, insert the data for the next hop, and calculate HMAC on the new data. Consequently, T_{crypt} for the hybrid scheme is $(5 + 4n)T_{mul} + 2(n + 1)T_{hash}$.

In [42], T_{mul} is found for an MNT curve, using 160 bits and an embedding degree of $k = 6$, equal to 0.6 $msec$. The Crypto++ library [43] is adpted to calculate T_{hash}, where it is compiled on an Intel Core2Duo 2 GHz machine. T_{hash} for SHA-1 is 0.21 μsec. Fig. 4.1 shows the cryptography delay in $msec$ vs. the number of intermediate nodes. It can be seen that the ESPR scheme significantly decreases the cryptography delay compared to that of the hybrid scheme. For example, when the number of intermediate nodes is 5, ESPR reduces the cryptography delay by more than 50% compared to that of the hybrid scheme.

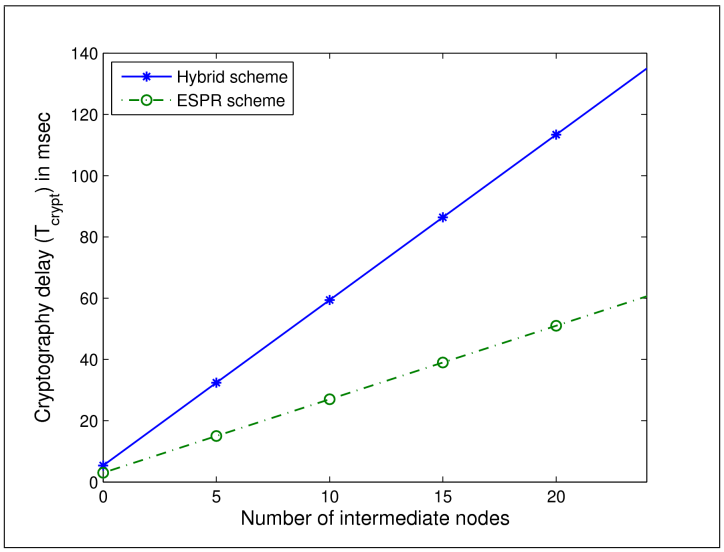


Figure 4.1: Cryptography Delay

4.3 Simulation-Based Performance Evaluation

To evaluate the performance of ESPR, a VANET scenario is designed and a number of simulations are developed. The goal of these simulations is to identify the effect of introducing ESPR on the network performance with respect to the end-to-end average delay, the effect of the number of intermediate nodes on that delay, the effect of the presence of some routing attacks on the network performance, and the corresponding performance with ESPR.

The scenario under consideration is for an ad hoc network between moving vehicles. Manhattan's city-street map is adopted to make the model realistic; also, a map based mobility model is applied. Vehicles are distributed randomly on the map's roads and they move with a maximum speed of $60km/hr$ toward random destinations during the simulation time. When a vehicle reaches an intersection, it changes its direction with probability of 0.5. The general simulation parameters are stated in Table 4.1

Table 4.1: General Parameters for ESPR Evaluating Simulations

Parameter	Value
Simulation Duration	30 sec
Simulation Area-Map	7.4 km x 7.4 km Manhattan City
Number of Vehicles	Varies
Mobility Model	Map Based
Speed of vehicles	$0 - 60$ km/hr
Transmission Range	300 m
Routing Protocol	GPSR
Beacon Interval	300 $msec$
Antenna	Omni antenna

4.3.1 End-to-End Delay

To evaluate the expected end-to-end delay for ESPR, an NS-2 [44] simulation is designed with respect to the previous simulation parameters, in addition to the simulation parameters in Table 4.2. The simulation has been repeated for different node densities in the simulation area. GPSR [10] is adopted as an example of the PBR scheme. First, the simulation is performed without any security overhead or cryptographic processes delay. Then, ESPR is considered to secure the GPSR protocol. After that, the simulation is repeated for the hybrid scheme[4] to demonstrate the superiority of ESPR.

Table 4.2: End-to-End Delay Simulation Parameters

Parameter	Value
Simulation software	$NS-2$ $Release$ 2.34
MAC protocol	$IEEE$ 802.11
Number of vehicles	$600, 1800, 2500, 3800$
Mobility model	Map Based, $TRANS$
Number of sources	10
Packet generation	Constant Bit Rate (CBR)
Packet generation interval	150 $msec$
Packet size	500 $bytes$

In order to estimate realistic performance evaluation results, cross layer protocols and real-word traffic models are deployed. GPSR is selected as the network layer routing protocol, and IEEE802.11 standard is adopted as the MAC layer protocol to approximate the IEEE 802.11p protocol. Finally, Omni antennas and 6 Mbps channel bandwidth are considered. For the mobility model and the different traffic scenarios, TraNS (Traffic and Network Simulation Environment) [45] is used to generate traffic scenario files compatible with the simulator NS-2.

The simulation results for the average end-to-end delay are shown in Table 4.3 for both ESPR and the hybrid security scheme, in addition to the average delay per packet for the same scenario without any security consideration. It is important to mention that in these simulations no attack is launched. The aim here is to identify the effect of the cryptography delay on the network performance with respect to the end-to-end delay. As cryptographic processes are performed at each intermediate node, the number of intermediate nodes has a significant effect on the end-to-end delay. Figure 4.2 shows the average end-to-end delay per packet in *msec* vs. the number of hops for GPSR, GPSR-ESPR, and GPSR-hybrid, respectively.

Table 4.3: Simulation Results for Average End-to-End Delay

Scheme	Average End-to-End Delay
GPSR	0.0282 *sec*
GPSR-ESPR	0.0412 *sec*
GPSR-Hybrid	0.0606 *sec*

Both ESPR and hybrid security schemes affect the network's performance in terms of end-to-end delay. However, ESPR introduces a notably smaller effect than the hybrid scheme. Thus, the cost to secure the multi-hop routing process in PBR is less with ESPR in terms of cryptography delay and, accordingly, the end-to-end delay.

This criterion is very critical for some VANETs applications. For example, the max-

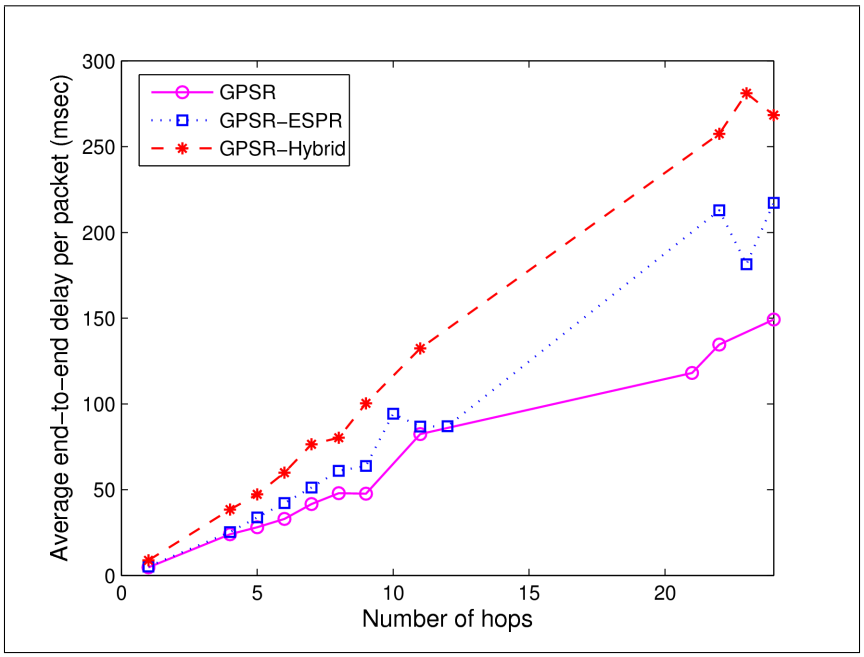


Figure 4.2: Average End-to-End Delay

imum allowed end-to-end delay for some safety applications is identified to be 100 *msec* [4]. In this simulation, more than 95% of the delivered packets are delivered within this limit for ESPR, while only 85.5% of the delivered packets with the hybrid scheme meet this constraint.

4.3.2 Resistance to Routing Attacks

A number of simulations are designed in order to evaluate the performance of the network with the presence of some predefined routing attacks. As illustrated in 4.1, ESPR is designed to detect and avoid most of the network layer attacks. ESPR guarantees that sending bogus information, modifying transmitted packets, or poisoning routing tables by external attackers are impossible. Routing loop, impersonation, sybil, and sinkhole attacks launched by external attackers are also impossible. Thus, external attackers can only replay legitimate packets; however, replay-based attacks, including wormhole attacks,

are detectable by ESPR.

Internal attacker, the attacker who has valid certificates and keys, is usually capable to launch some routing attacks. The cryptographic properties of ESPR enable the traceability of an internal attacker who originates and injects falsified information in addition to the detection of any multi-hop packet modification. In other routing attacks, internal attackers announce falsified position information, drop forwarded packets, or cause routing loops. The set of plausibility checks in ESPR are designed to detect these attacks and report the suspicious nodes to the TA.

A set of simulation scenarios has been developed to evaluate the impact of different routing attacks on the packet delivery rate (PDR). The same city-scenario in section 4.3 and the general simulation parameters in Table 4.1 are considered. In this set of simulations, a perfect wireless channel access is assumed as it is targeted to evaluate the packet loss due to routing layer factors. The simulation parameters are listed in Table 4.4 and the full set of simulation results are presented in Table 4.5.

Table 4.4: Parameters for The Routing Attacks Simulation

Parameter	Value
Simulation software	MATLAB 7.4
MAC protocol	ideal
Number of vehicles	$10 - 100$ $vehicles/km^2$
Mobility model	Map Based
Number of sources	5
Packet generation interval	150 $msec$
Overhearing hold interval	600 $msec$
Repetition	10 / scenario

Impact of ESPR on an Attack-Free Network

In this simulation, no attack is launched in the network. The performance of the network with the GPSR protocol is first measured by means of the packet delivery rate (PDR). Then the performance of the network is evaluated when ESPR is implemented into the routing protocol . Figure 4.3 shows the variance in performance between GPSR and ESPR-GPSR in an attack-free scenario.

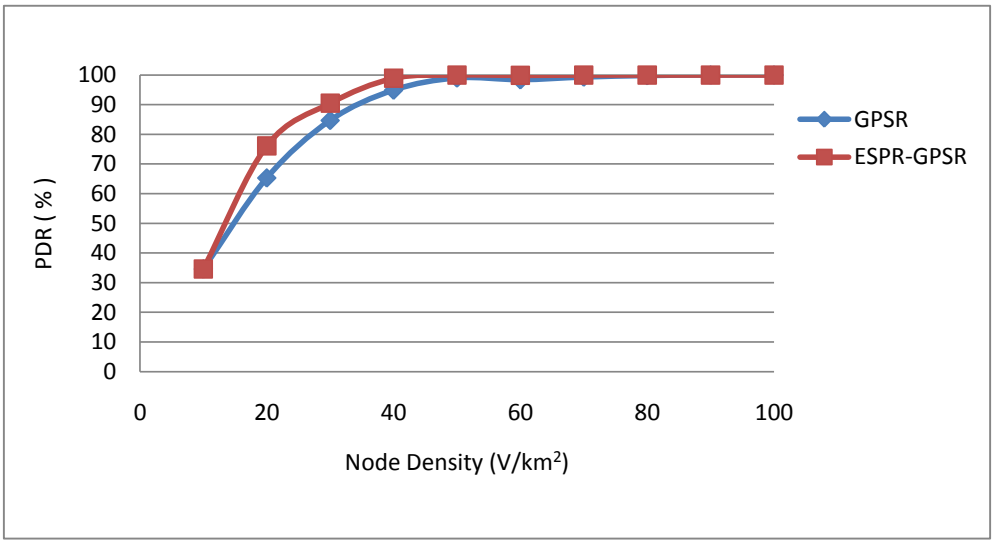


Figure 4.3: Effect of ESPR on PDR: Attack-Free Scenario

The graph shows that ESPR-GPSR outperforms GPSR in terms of PDR; the overhearing procedure in ESPR gives packets new opportunities to be delivered via other paths when they are not overheard. In an attack-free network, packets are not overheard if there is a link-breakage, a lack of neighbours, or if a packet reaches back to the same location that it has entered in the perimeter-mode. In this simulation, a link between two nodes is broken if the distance between them became greater than the node's transmission range during the processing delay. In this scenario, the slight improvement in the network performance is mainly due to the duplicated packets generated by the overhearing procedure.

Moreover, it is important to notice that putting the suspicious nodes on hold for the time interval specified in Table 4.4 does not degrade the PDR even with low vehicle densities.

Impact of Routing Loop Attack

In routing loop attack, an internal attacker receives a massage, updates it, and sends it back to one of the previous forwarders (or the source) even if there is a better node in its routing table that is available to be the next forwarder according to the routing strategy. The aim of this attack is to delay or prevent the delivery of a massage. The attack could also consume the bandwidth. To evaluate the impact of this attack on the network's PDR, a simulation scenario was designed and both GPSR and ESPR-GPSR routing were applied. In this simulation, an attacker ignores the routing strategy and sends the packet back to its sender. The ESPR strategy and content checks are designed to evaluate received packets in order to detect such misbehaviour with respect to the GPSR's routing modes. Figure 4.4 and 4.5 show the simulation results for the impact routing loop attacks have on an unsecured network with diffrent proportions of attackers, and the corresponding impact when ESPR is incorporated into the routing protocol, respectively.

Impact of Sinkhole Attack

In a sinkhole attack, an internal attacker convinces other nodes to be their next hop forwarder by announcing a different location in its beacon messages; it then drops any received message in a selfish behaviour. The impact of sinkhole attacks on the network performance includes both poisoning the routing tables of the attacker's neighbours and dropping their packets. A sinkhole attacker can be rational or irrational according to its motive. Rational sinkhole attackers aim to grab other node packets to analyze them. For example, an attacker will claim a location close to an automatic payment unit in order to

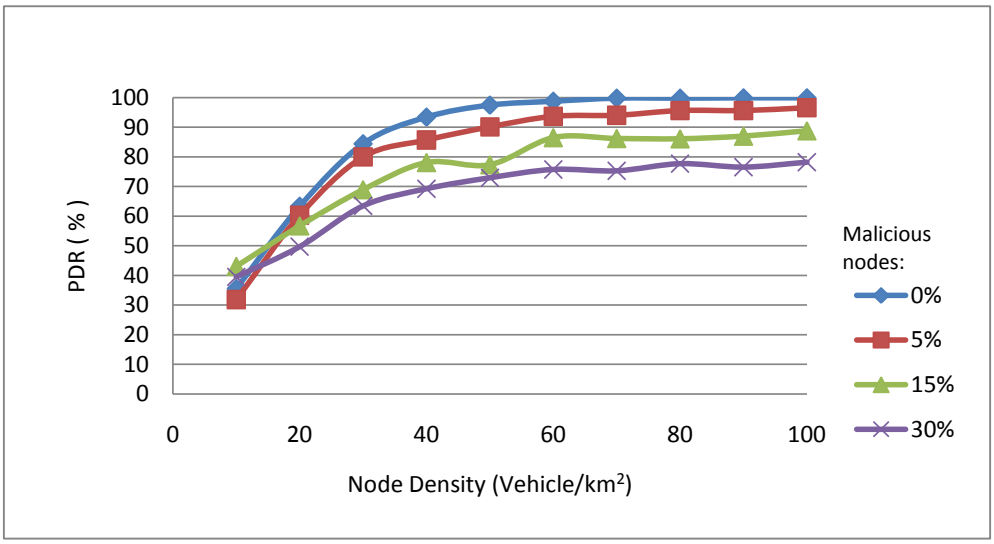


Figure 4.4: Impact of the Routing Loop Attack on PDR

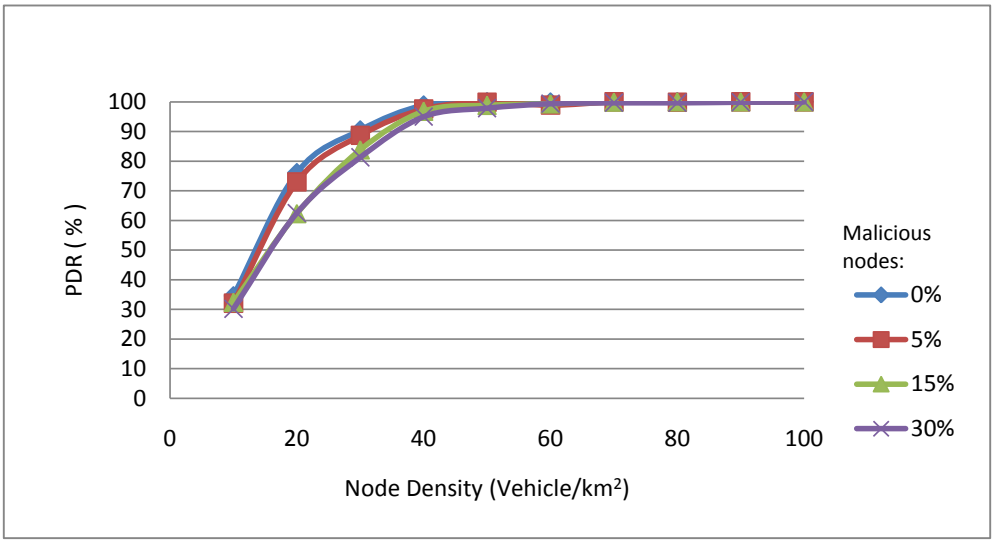


Figure 4.5: ESPR Resistance to Routing Loop Attack

extract important payment information. On the other hand, irrational sinkhole attackers aim to disturb the network operation.

Two sets of simulations are developed to evaluate the impact of sinkhole attacks. In the first set, a proportion of the scenario's nodes are selected to be the attackers. Each

attacker claims random locations in its beacon messages and drops any received message. In the second set of simulations, the attack is designed in such a way that the attacker claims a plausible location located on the road map and within its transmission range. The claimed location was designed to be ahead of the real attacker's location by the value $R/2$ in its movement direction, where R is the transmission range. This attack is referred to as smart sinkhole attack.

Figures 4.6 and 4.7 show the PDR for scenarios involved simple sinkhole attack and smart sinkhole attack, respectively. It can be seen that the simple sinkhole attack affects the PDR of the network more than the smart sinkhole attack. By claiming farther distances, the simple sinkhole attackers are able to convince more nodes to be their next hop; the smart sinkhole attackers limit their location options in order to be plausible.

Vehicles with ESPR plausibility check set are able to detect sinkhole attacks autonomously and maintain the PDR of the network. Figure 4.8 shows the corresponding network PDR when ESPR is implemented into the routing protocol. The GPSR-ESPR curve is very close to the attack-free PDR curve, with respect to losing 15% of the vehicles due to their uncooperative behaviour.

Impact of Wormhole Attack

In a wormhole attack, two or more attackers are connected via a private high speed link and they resend messages heard in one terminal into the other terminal(s). Replaying authentic beacons from different locations enables attackers to dominate the routing paths. Wormhole attackers connect the network via their private connection, which may improve the network's performance as if RSUs have been used for this purpose. However, the attackers aim is to dominate the connection so they can eavesdrop or partition the network.

The first simulation set is designed to evaluate the network's PDR when attackers replay any packet heard in any site. As attackers are replaying beacons, nodes in the

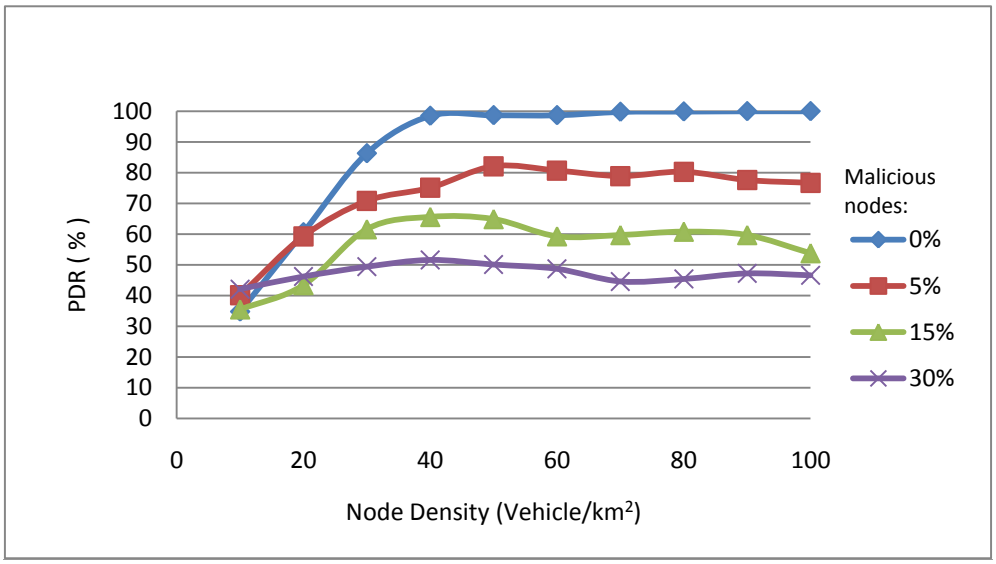


Figure 4.6: Impact of the Simple Sinkhole Attack

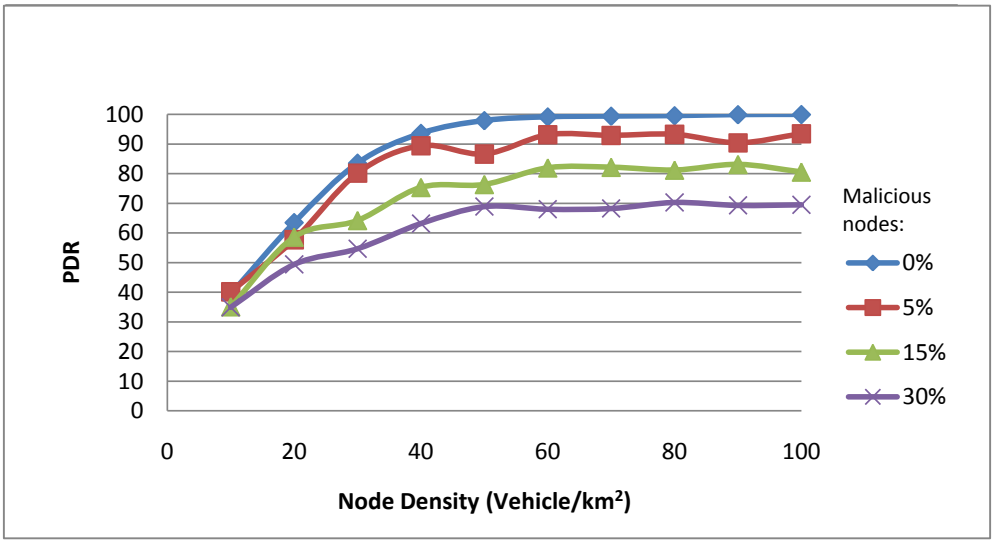


Figure 4.7: Impact of the Smart Sinkhole Attack

attackers' transmission range hear authentic beacons from different sites; thus, have larger routing tables. When a node sends a packet to another node in its routing table but not within its transmission range, the packet will be replayed in the other sites by the attackers and will be received by the targeted node. Figure 4.9 shows the effect of this

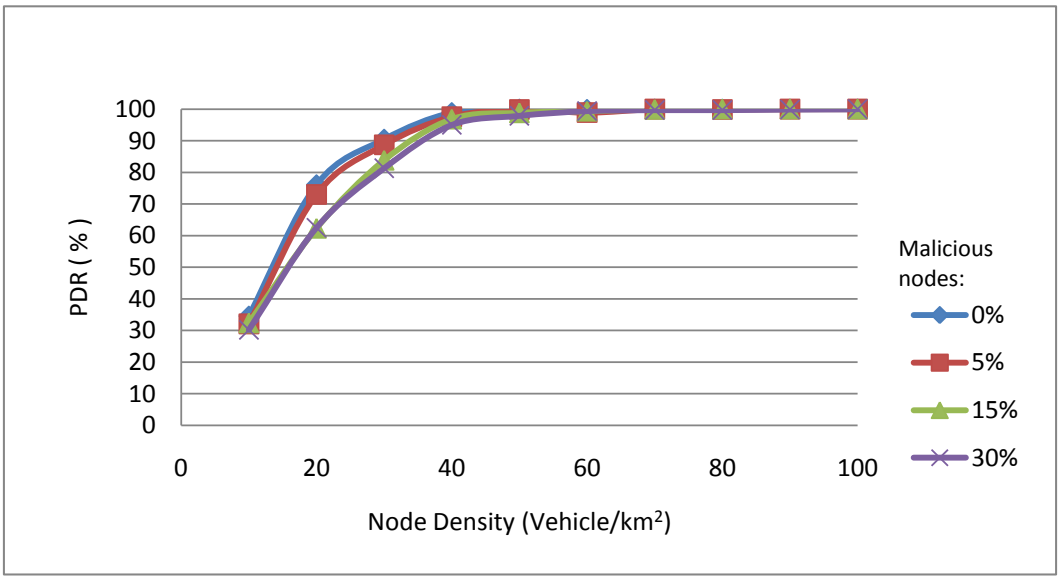


Figure 4.8: ESPR Resistance to Sinkhole Attack

attack on the PDR. This attack has to be detected and avoided in order to avoid both packet analysis and network congestions. Figure 4.10 shows the corresponding PDR when ESPR is implemented into the routing protocol.

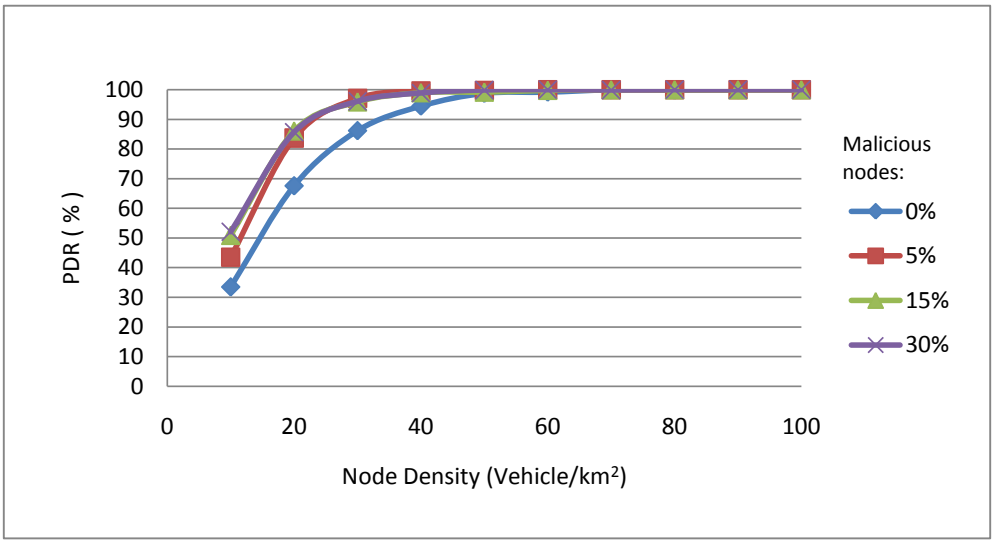


Figure 4.9: Impact of the Wormhole Attack

In the second simulation set, the attackers are designed to disconnect the network by

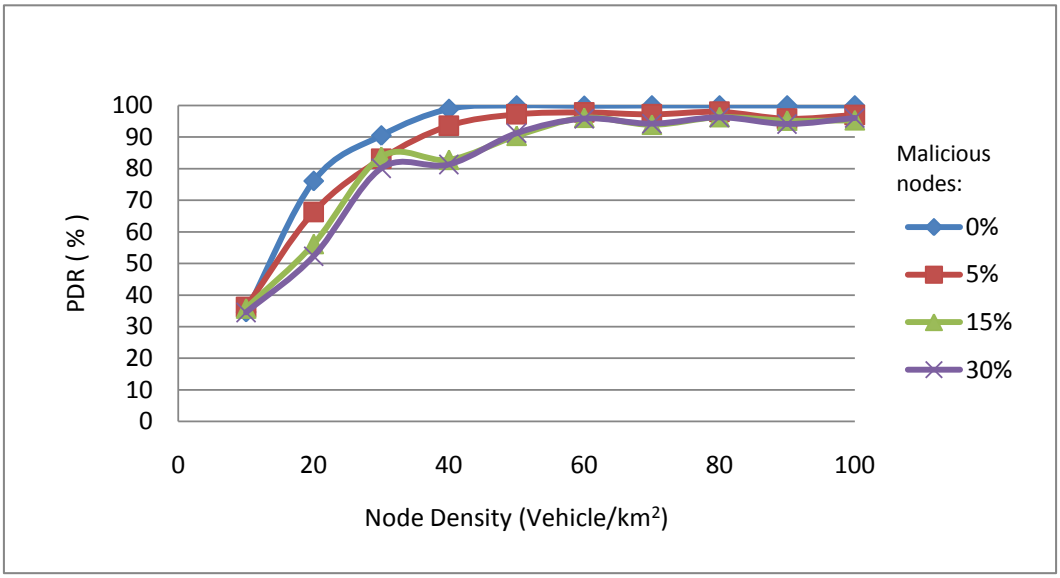


Figure 4.10: ESPR Resistance to Wormhole Attack

replaying beacon messages and dropping other packets. Figure 4.11 shows the effect of this attack on an unsecured network. Figure 4.12 shows the corresponding PDR when ESPR is employed. ESPR enables the routing protocol to resist this kind of attacks and maintain the network's PDR.

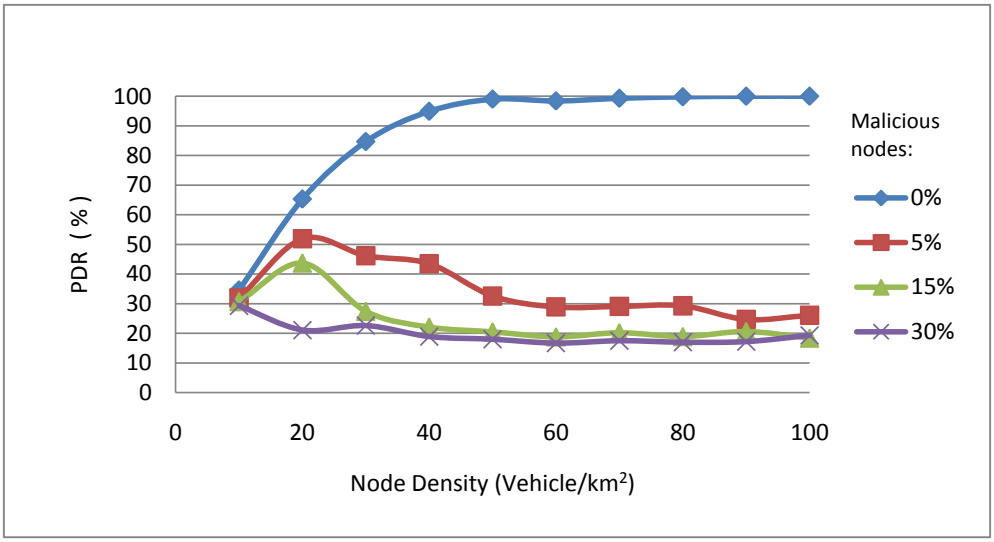


Figure 4.11: Impact of the Wormhole attack whith Packet Dropping

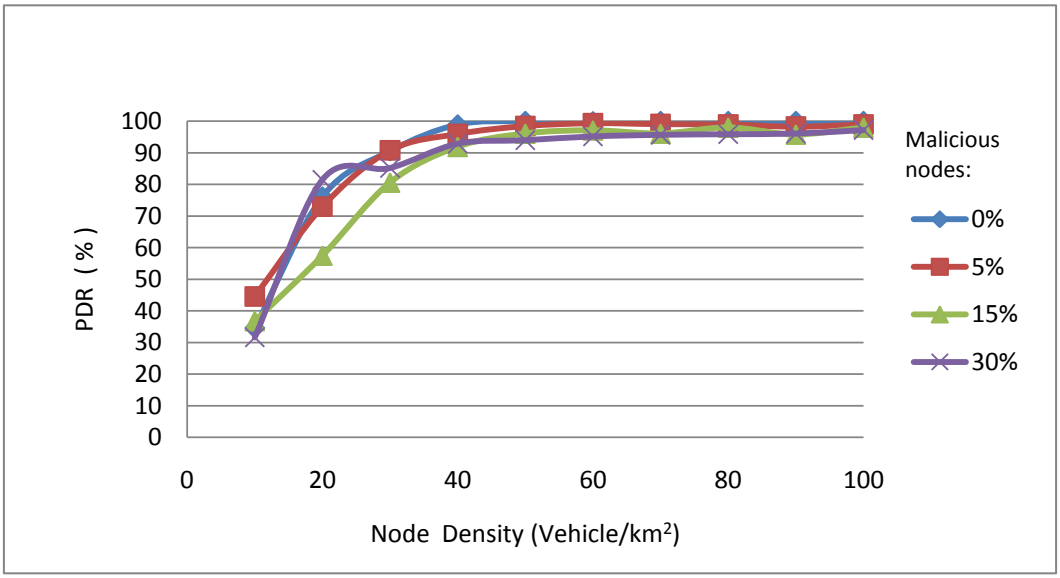


Figure 4.12: The ESPR Resistance to Wormhole Attack with Packet Dropping

Table 4.5: The Results of Routing Attacks Simulations

Attack	Proportion	PDR (%)/ Node Density (v/km^2)									
		10	20	30	40	50	60	70	80	90	100
Attacks-free		34.6	76.1	90.5	98.9	100	99.9	100	100	100	100
Sinkhole	5%	29.3	59.9	91.1	98.4	99.5	100	100	99.9	100	100
	15%	29.3	56.9	80.8	96.3	98	99.9	99.6	100	99.9	100
	30%	40.3	47.9	69.8	84.8	94.6	97.6	99.1	99.8	99.9	100
Smart Sinkhole	5%	34.5	69.3	92.4	97.5	98.7	99.9	100	100	100	100
	15%	22.7	66.7	86.9	96.2	98.9	99.4	99.6	99.9	100	100
	30%	23.8	45.3	77.5	88.9	94.1	99.1	98.8	99.5	99.9	100
Wormhole	5%	36.2	66.3	83.1	93.6	97.2	97.8	97.2	98	95.8	97
	15%	35.8	56.2	83.8	82.8	90.4	96.1	93.9	96.3	95.2	95.3
	30%	34.5	52.3	80.1	81.3	91.2	95.8	94.2	96.2	94.1	96
Wormhole with dropping	5%	44.6	73	90.8	96	98.5	99.4	99.1	99	98.3	99
	15%	36.8	57.5	80.6	91.9	96.1	97.1	96.1	98	95.8	98
	30%	31.6	81.5	85.2	92.9	94	95.2	95.7	95.9	96.1	97.2
Routing loop	5%	32.1	73	88.7	97.6	99.9	98.9	100	99.9	100	100
	15%	32.4	62.3	83.8	96.8	98.8	99.3	99.9	100	100	100
	30%	30.2	62.5	81.3	95	97.9	99.4	99.7	99.7	99.9	100

4.3.3 Discussion

All the conducted simulation results support the analysis provided in previous sections. The results show that ESPR secures PBR at the cost of some extra end-to-end delay. ESPR is capable of detecting and recovering from routing attacks, even when the attackers are internal.

In the first simulation environment, a realistic scenario with cross-layer standards was applied to precisely identify end-to-end delay. Cryptographic processes, applied at each intermediate node, result in a major increase to the end-to-end delay; however, this delay is less than the delay resulting from other schemes to achieve the same level of security. The analysis shows that ESPR decreases the cryptography delay by half compared to the hybrid scheme's cryptography delay, and the simulation results support that. The results also show a relation between the number of intermediate nodes involved in delivering a packet, and the average end-to-end delay: increasing the number of intermediate forwarders significantly increases the average end-to-end delay. The designed simulation considered the worst case in terms of the involved intermediate forwarders to deliver packets in the Manhattan-city model, as it did not employ any fixed infrastructure to connect the network.

The second simulation environment was designed to evaluate the PDR of the network in the presence of routing attacks. Routing attacks threaten the network performance even with the presence of a cryptographic security scheme. The simulation considered the normal behaviour of well-known attacks. Neither of the simulation scenarios considered attackers with directional antennas or cooperative sinkhole attackers.

The overhearing procedure was designed in such a way that the node retransmits the packet to the next forwarder in its routing table if the transmission of the packet was not detected from the current forwarder. Then, the sender puts the suspicious nodes on hold for a predefined time interval, i.e., the sender does not consider the suspicious node for routing purposes for a period of time. In some cases, a packet is dropped due to a routing

decision, and then another version of the packet is transmitted. Therefore, overhearing slightly improves PDR at the cost of injecting redundant packets to the network. Packets are retransmitted until reaching their destinations or expiry time. The hold interval, the impacts of the redundant packets, and the packets life-time are important issues in the proposed overhearing scheme; they need to be studied and optimized.

Although the results indicate high PDR in ESPR, it is expected that ESPR has better performance in a real life setting. The simulation scenarios only considered autonomous detection of attackers. When a node detects a malicious behaviour, e.g., a legitimate node claiming a falsified-position, the detector avoids cooperation with this node. The rest of the ESPR procedure was not considered in the simulation. The detector should report misbehaviour to the TA, then the TA have to send a revocation message to alert all the legitimate nodes about an attacker's identity. Thus, the real scenario leads to a faster adversaries' disclosure and a better PDR. The time taken to detect an attacker, report its behaviour, and distribute a revocation message was also not considered in this simulation.

Section 4.3.2 presents the impact of different routing attacks on a PBR-based VANET. The simulation scenario is under the assumption that the network is secured by cryptographic means and that the attackers are internal. The set of simulations are designed to emphasize the importance of the plausibility checks in ESPR. The results show that the PDR is significantly decreased when there is an absence of plausibility checks. The wormhole attack with packet dropping behaviour has the worst PDR, because the attackers use many legitimate beacons to fool their neighbours. Routing loop attack has the least impact on PDR, because it does not include falsified-position information or packet dropping behaviour in the designed scenario. Wormhole attack remarkably increases the PDR as it connects the network; however, this improvement should be done in a formal scheme and not by anonymous attackers. For example, similar improvement can be achieved by using fixed RSUs as gateways to the infrastructure, under the supervision of the TA.

The results also show the resistance of ESPR's plausibility checks to different routing attacks. The PDR is closly resembles the attack-free scenario in most cases, taking into consideration losing a portion of the network density. The wormhole scenarios have a slightly lower PDR, this is because nodes detect beacons with implausible locations in their transmission range. Thus, detecrors stop cooperation with the suspicious nodes for the rest of the simulation interval. The effect increases with longer simulation time. However, nodes should report these suspicious beacons to the TA and wait for the revocation messages. The TA will be able to recognize the wormhole attack according to the reported messages.

4.4 Summary

In this chapter, the proposed ESPR was evaluated in terms of security and bit-size. The proposed cryptography scheme supports the network through primary security requirements. The corresponding key management scheme guarantees secure delivery of the required security materials and forward secrecy. This chapter included detailed analysis of the communication overhead and the cryptography delay added by ESPR, in addition to a simulation-based evaluation.

Table 4.6 summarizes the ESPR resistance to the different routing attacks delivered by analysis and simulation results. Impossible attack means that ESPR guarantees the detection of it autonomously. Detectable attacks can be discovered by some nodes in the network; autonomous detection by all nodes is not guaranteed. When an attacker has been detected and reported, the TA broadcasts a revocation message to disclose its identity. The simulation results show that ESPR enables the network member to detect routing attacks and maintain a high PDR.

ESPR provides the required security for the network on the cost of some cryptographic operations and logical checks. The cryptographic operations introduce both processing

Table 4.6: Parameters for The Routing Attacks Simulation

Attack	External	Internal
Injuction of bogus information	Impossible	Traceable
Payload modification	Impossible	Impossible
Identity impersonation	Impossible	Impossible
Replay	Detectable	Detectable
Routing loop	Impossible	Detectable
Claiming falsified location information	Impossible	Detectable
Wormhole	Detectable	Detectable
Sybil	Impossible	Impossible
Sinkhole	Impossible	Detectable

delay and communication overhead. The overhead incurred by ESPR is 185 *bytes*, which is 43.9% less than the corresponding overhead incurred by the hybrid scheme, that provides the same level of security. Moreover, the cryptography delay introduced by ESPR is lower compared to that of the hybrid scheme. The simulation results support our analysis.

Chapter 5

Conclusions and Future Work

The conducted research of this thesis is summarized and concluded in this chapter, followed by the future work.

5.1 Summary

ESPR is a novel security scheme developed by the author to secure PBR protocols in the VANETs context. In PBR, vehicles cooperate to deliver the network packets using distributed routing, where routing decisions are taken by intermediate forwarders with respect to the location of the forwarder, its neghbouring nodes and the destination vehicle. Securing PBR protocols requires both hop-by-hop and end-to-end security. ESPR guarantees originator authentication, data integrity, and end-to-end non-repudiation through its cryptographic scheme. In ESPR, each message originator signs the message with its private key. In multi-hop applications, legitimate forwarders update the mutable fields of a message and recalculate HMAC value using a shared secret key. Each recipient verifies the HMAC value, and then the originator's signature.

ESPR uses a novel key management system to manage the distribution, revocation, and key renewal processes. PKI with ECDSA is applied as a public key environment. A probabilistic key distribution is also applied with a hash chain-based technique to manage the symmetric shared key. The proposed scheme guarantees secure key management and forward secrecy.

ESPR also defines a set of plausibility checks that enable vehicles to detect and avoid routing attacks. The checks are run autonomously and the detection is not fully guaranteed; however, the analysis and the simulation results conclude a high detection level.

Both analysis and simulation results demonstrate that ESPR outperforms its counterparts. The reduction in the cryptographic processes at each intermediate node significantly reduces the end-to-end delay required to deliver a message. Moreover, the bit-size added by ESPR for security purposes is noticeably small in respect to the provided level of security.

5.2 Contributions

The major contributions of this thesis can be summarized as follows:

- PBR attacks have been studied. Some of these attacks have been implemented and simulated in a VANET environment, and their impact on the packet delivery rate (PDR) has been studied.
- A cryptographic scheme has been proposed to secure PBR protocols. This scheme has less cryptography delay and less communication overhead than its counterparts that have equal security strength.
- A key management scheme has been proposed to manage the required keys by ESPR. This scheme describes the security materials required and the techniques applied to maintain the operation of ESPR.

- A set of plausibility checks has been proposed. This set includes applying the Greenshield model to the location verification problem.

5.3 Future Work

ESPR introduces significant progress to the security of PBR in VANETs; however, this field still requires more research. In following, several issues are provided to further enhance the field.

Impact of privacy solutions on PBR

For privacy purposes, vehicles chance their identities frequently. This affects the performance of PBR-based systems. The impact of changing vehicles identities on the network performance need to be studied in order to optimize the life-time of each identity, in case of using multiple anonymous identities, or find new privacy solutions that perform well with the PBR context.

Optimization issues for the overhearing procedure

In ESPR, nodes keep track of their packets' transmission by the next forwarders. When a node does not detect the transmission, it avoids sending messages to that node for a period of time, and retransmits the packet to another forwarder instead. This procedure needs an extensive study. The hold period can be optimized for better system performance. In addition, the impact of retransmission on the network needs to be investigated. The study may consider many factors such as node density and network congestions.

Resistance to signature jamming attacks

ESPR can easily detect and avoid the signature jamming attack (SJA) because it first verifies the HMAC value. This attack was not considered in this thesis. Further investigation on SJA, and corresponding resistance of ESPR are feasible.

Adaptive ESPR

In ESPR, the major end-to-end delay is consumed to verify the source's signature. As ESPR introduces another level of trust, having the shared secret key, intermediate nodes in multi-hop packets can verify an originator's signature with a variable probability. Thus, the end-to-end delay will significantly be reduced. As a forwarder does not obtain any information from the forwarded packets, the network is vulnerable only to packet injection attack by internal adversaries. Thus, the probability of verification can be related to the traffic density in the network and the detection of attackers.

Improved GSIS for PBR

In GSIS [26], the authors propose group signature and identity-based signature to meet the security requirements and reduce the cryptography overhead. However, GSIS does not consider the multi-hop problem or protect the network from the routing attacks. The techniques that used in ESPR to overcome these problems can be deployed to improve the GSIS.

Bibliography

[1] Car2car communication consortium. [Online]. Available: `http://www.car-to-car.org`. 2, 18

[2] M. Raya and J.P. Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007. 2, 13, 17, 19, 20, 28

[3] ASTM E 2213-03. Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems-5GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *ASTM International.*, 2003. 2, 18

[4] C. Harsch, A. Festag, and P. Papadimitratos. Secure position-based routing for VANETs. In *2007 IEEE 66th Vehicular Technology Conference, 2007. VTC-2007 Fall*, pages 26–30, 2007. 3, 19, 21, 22, 23, 25, 56, 57, 60, 62

[5] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, pages 90 –100, 25-26 1999. 7

[6] D.B. Johnson. Routing in ad hoc networks of mobile hosts. In *Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on*, pages 158 –163, 8-9 1994. 7

[7] F. Li and Y. Wang. Routing in vehicular ad hoc networks: A survey. *Vehicular Technology Magazine, IEEE*, 2(2):12 –22, june 2007. 8, 10, 12

[8] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz. CarTALK 2000: Safe and comfortable driving based upon inter-vehicle-communication. In *IEEE Intelligent Vehicle Symposium, 2002*, volume 2, 2002. 8

[9] A. Festag, G. Noecker, M. Strassberger, A. Lubke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch. NoW-Network on Wheels: Project Objectives, Technology and Achievements. In *Proc. 5th International Workshop on Intelligent Transportation*, pages 211–216, 2008. 8, 19

[10] B. Karp and HT Kung. GPSR: greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254. ACM, 2000. 8, 10, 60

[11] Y.B. Ko and N.H. Vaidya. Location-Aided Routing (LAR) in mobile ad hoc networks. *Wireless Networks*, 6(4):307–321, 2000. 10

[12] L. Blazevic, S. Giordano, and JY Le Boudec. Self organized terminode routing. *Cluster Computing*, 5(2):205–218, 2002. 10

[13] W.H. Liao, J.P. Sheu, and Y.C. Tseng. GRID: A fully location-aware routing protocol for mobile ad hoc networks. *Telecommunication Systems*, 18(1):37–60, 2001. 10

[14] C. Lochert, M. Mauve, H. Fuler, and H. Hartenstein. Geographic routing in city scenarios. *ACM SIGMOBILE Mobile Computing and Communications Review*, 9(1):72, 2005. 10

[15] J. Tian, L. Han, K. Rothermel, and C. Cseh. Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks. In *Proc. of the IEEE 6th Intl. Conf. on Intelligent Transportation Systems (ITSC*, volume 2, pages 1546–1551, 2003. 10

[16] V. Naumov and TR Gross. Connectivity-aware routing (CAR) in vehicular ad-hoc networks. In *IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, pages 1919–1927, 2007. 11

[17] B.C. Seet, G. Liu, B.S. Lee, C.H. Foh, K.J. Wong, and K.K. Lee. A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications. *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*, pages 989–999, 2004. 11

[18] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter. MDDV: a mobility-centric data dissemination algorithm for vehicular networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, page 56. ACM, 2004. 11

[19] Y. Ding, C. Wang, and L. Xiao. A static-node assisted adaptive routing protocol in vehicular networks. In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, page 68. ACM, 2007. 11

[20] T. Taleb, M. Ochi, A. Jamalipour, N. Kato, and Y. Nemoto. An efficient vehicle-heading based routing protocol for VANET networks. In *Proc. IEEE WCNC*, volume 6. 12

[21] B.K. Chaurasia and S. Verma. Maximizing anonymity of a vehicle through pseudonym updation. In *Proceedings of the 4th Annual International Conference on Wireless Internet*, pages 1–6. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008. 18

[22] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos. Impact of pseudonym changes on geographic routing in VANETs. *Security and Privacy in Ad-Hoc and Sensor Networks*, pages 43–57. 18

[23] J.P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, 2(3):49–55, 2004. 18

[24] The secure vehicle communication (sevecom) project. [Online]. Available: `http://www.sevecom.org/`. 18

[25] C.I. Fan, R.H. Hsu, and C.H. Tseng. Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks. In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, page 82. ACM, 2008. 19

[26] X. Lin, X. Sun, P.H. Ho, and X. Shen. GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 56(6 Part 1):3442–3456, 2007. 19, 20, 79

[27] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmuller. Attacks on inter vehicle communication systems-an analysis. In *International Workshop on Intelligent Transportation (WIT)*. Citeseer, 2006. 20

[28] T. Leinmuller, C. Maihfer, E. Schoch, and F. Kargl. Improved security in geographic ad hoc routing through autonomous position verification. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, page 66. ACM, 2006. 20

[29] S. Capkun and J.P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, 2006. 21

[30] N. Abu-Ghazaleh, K.D. Kang, and K. Liu. Towards resilient geographic routing in WSNs. In *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, page 78. ACM, 2005. 21

[31] J.H. Song, V.W.S. Wong, and V.C.M. Leung. Secure location verification for vehicular ad-hoc networks. In *IEEE Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008*, pages 1–5. Citeseer, 2008. 21

[32] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Network and Distributed System Security Symposium (NDSS)*, pages 131–141. Citeseer, 2004. 21

[33] D. Johnson, A. Menezes, and S. Vanstone. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001. 28, 57

[34] W.M. Daley, R.G. Kammer, BOOZ-ALLEN, and HAMILTON INC MCLEAN VA. Digital Signature Standard (DSS). 2000. 29

[35] A. Wasef and X.S. Shen. MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks. *IEEE GLOBECOM*, 2009. 29, 39, 43

[36] D. Eastlake and P. Jones. US secure hash algorithm 1 (SHA1). *RFC 3174*, Sept. 2001. 29, 57

[37] J.J. Haas, Y.C. Hu, and K.P. Laberteaux. Design and analysis of a lightweight certificate revocation mechanism for VANET. In *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*, pages 89–98. ACM, 2009. 39

[38] H. Zhu, R. Lu, X. Shen, and X. Lin. Security in service-oriented vehicular networks. *IEEE Wireless Communications*, 16(4):16–22, 2009. 39

[39] S. Zhu, S. Setia, S. Xu, and S. Jajodia. GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks. *Journal of Computer Security*, 14:301–325, 2006. 41, 43

[40] M. Scott. Efficient implementation of crytographic pairings. In *[Online]. http://www. pairing-conference. org/2007/invited/Scott slide. pdf.* 47

[41] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-Reductions. *IEIC Technical Report (Institute of Electronics, Information and Communication Engineers)*, 100(323(ISEC2000 58-67)):99–108, 2000. 57

[42] M. Scott. Computing the Tate pairing. *Topics in Cryptology, Springer*, pages 293–304, 2005. 58

[43] Crypto++ library 5.5.2. Available: `http://www.cryptopp.com/`. 58

[44] The network simulator - ns-2. Available: `http://nsnam.isi.edu/nsnam/index.php/UserInformation`. 60

[45] Traffic and network simulation environment - TraNS. Available: `http://trans.epfl.ch/`. 61

[46] H. Miranda and L. Rodrigues. Reputation in anonymous vehicular networks. *International Journal of Autonomous and Adaptive Communications Systems*, 3(2):178–197, 2010.

[47] S. Eichler. A security architecture concept for vehicular network nodes. *Proc. 6th International Conference on Information, Communications & Signal Processing*, pages 1–5, 2007.