SECURE LOCALIZATION TOPOLOGY AND METHODOLOGY FOR A DEDICATED AUTOMATED HIGHWAY SYSTEM

by

Bhaswati Deka

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Electrical Engineering

Approved:

Dr. Ryan M. Gerdes Major Professor	Dr. Edmund Spencer Committee Member
Dr. Doran J. Baker Committee Member	Dr. Mark R. McLellan Vice President for Research and Dean of the School of Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2013

Abstract

Secure Localization Topology and Methodology for a Dedicated Automated Highway System

by

Bhaswati Deka, Master of Science

Utah State University, 2013

Major Professor: Dr. Ryan M. Gerdes
Department: Electrical and Computer Engineering

Localization of nodes is an important aspect in a vehicular ad-hoc network (VANET). Research has been done on various localization methods. Some are more apt for a specific purpose than others. To begin with, we give an overview of a vehicular ad-hoc network, localization methods, and how they can be classified. The distance bounding and verifiable trilateration are explained further with their corresponding algorithms and steps used for localization. Distance bounding is a range-based distance estimation algorithm. Verifiable trilateration is a popular geometric method of localization. A dedicated automated highway infrastructure can use distance bounding and/or trilateration to localize an automated vehicle on the highway. We describe a highway infrastructure for our analysis and test how well each of the methods performs, according to a security measure defined as spoofing probability. The spoofing probability is, simply put, the probability that a given point on the highway will be successfully spoofed by an attacker that is located at any random position along the highway. The spoofing probability depends on different quantities depending on the method of localization used. We compare the distance bounding and trilateration methods to a novel method using friendly jamming for localization. Friendly jamming works by creating an interference around the region whenever communication takes place between

a vehicle and a verifier (belonging to the highway infrastructure, which is involved in the localization process using a given algorithm and method). In case of friendly jamming, the spoofing probability depends both on the position and velocity of the attacker and those of the target vehicle (which the attacker aims to spoof). This makes the spoofing probability much less for friendly jamming. On the other hand, the distance bounding and trilateration methods have spoofing probabilities depending only on their position. The results are summarized at the end of the last chapter to give an idea about how the three localization methods, i.e. distance bounding, verifiable trilateration, and friendly jamming, compare against each other for a dedicated automated highway infrastructure.

We observe that the spoofing probability of the friendly jamming infrastructure is less than 2% while the spoofing probabilities of distance bounding and trilateration are 25% and 11%, respectively. This means that the friendly jamming method is more secure for the corresponding automated transportation system (ATS) infrastructure than distance bounding and trilateration. However, one drawback of friendly jamming is that it has a high standard deviation because the range of positions that are most vulnerable is high. Even though the spoofing probability is much less, the friendly jamming method is vulnerable to an attack over a large range of distances along the highway. This can be overcome by defining a more robust infrastructure and using the infrastructure's resources judiciously. This can be the future scope of our research. Infrastructures that use the radio resources in a cost effective manner to reduce the vulnerability of the friendly jamming method are a promising choice for the localization of vehicles on an ATS highway.

(75 pages)

Public Abstract

Secure Localization Topology and Methodology for a Dedicated Automated Highway System

by

Bhaswati Deka, Master of Science

Utah State University, 2013

Major Professor: Dr. Ryan M. Gerdes
Department: Electrical and Computer Engineering

In today's fast-paced world, mobility is a very important factor in improving the quality of living. The purpose of an automated transportation system (ATS) is to provide mobility to one and all, irrespective of their capabilities. An ATS requires a lot of planning to be efficient and safe for public use. One of the main aspects of safety is to determine the location of the individual vehicles within the system and ensure that their location is not posing any hazard to other vehicles in the system or any other entity outside the system. The process of determining or verifying the position of a particular object in space is called localization. In an automated driverless vehicle, localization not only needs to be accurate but also secure. This is because an adversary may be able to use the position of an automated vehicle for malicious activities and disrupt normal functioning of the system. Therefore, it is not only important, but also necessary, to create a secure localization system for any ATS. This is the motivation of our research on vehicular localization methodology and topology. We compare two existing localization methods called distance bounding and verifiable trilateration with a novel method using friendly jamming for the specific case of a dedicated automated highway. A dedicated highway consists of lanes exclusively for use by automated vehicles. Individual units belonging to the highway infrastructure called verifiers

are placed on, or surrounding, the highway according to a planned scheme. These verifiers securely implement the process of localization.

The introduction gives a brief account of ATS and its current relevance. We delve into some theory related to localization, and in the later part of this section, the probability theory required for our analysis is reviewed. Then we discuss the infrastructures on which we study the effectiveness of the three methods mentioned earlier. Here, the focus is on a dedicated automated highway infrastructure. After defining the infrastructures, we find the segments of the highway that are prone to attacks and describe an approach based on probability theory to analyse the vulnerability of a given infrastructure. The term used for the measure that tells us about the security of a given infrastructure using a given localization method is spoofing probability. In the corresponding chapter, the formulae used to arrive at the expressions for spoofing probability are derived. The spoofing probability plots are generated for each method under different circumstances and compared. Before we explain spoofing probability, we have a chapter in which the novel idea of friendly jamming and its application in an ATS is explained.

We observe that the spoofing probability of the friendly jamming infrastructure is much less than that for distance bounding and trilateration. This means that the friendly jamming method is more secure for the corresponding ATS infrastructure than distance bounding and trilateration. However, one drawback of friendly jamming is that it is vulnerable to attack over a large range of distances along the highway, even though the spoofing probability is much less. This can be overcome by defining a more robust infrastructure and using the infrastructure's resources judiciously. Our research can be continued further along these lines.

Acknowledgments

I wish to thank those who have helped me in this process, from embarking on a research topic to defending my thesis and completing the final draft. I thank my major professor, Dr. Ryan Gerdes, my committee members, Dr. Edmund Spencer and Dr. Doran Baker, and Dr. Kevin Heaslip from TIMELab, USU, for giving me candid reviews and instilling confidence in me to carry out better research work. I am enormously thankful to Dr. Gerdes for his patience with me whenever I was lagging behind and for being a very approachable mentor. I am thankful to my parents, Amiya Kumar Deka and Runuma Deka, for having faith in me and allowing me to pursue my interests, and my brother, Om, for inspiring me through his way of life. I thank my friends Amrita, Shantanu, Saptarshi, and Vishal Sharma for extending their help during my thesis defense, and Jval and Manish for keeping me focused with their positive talks. I thank Chiranjeev for being a good listener and his tacit support as I worked towards my goals.

Bhaswati Deka

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Intelligent Transportation System (ITS)

With the advent of computing and communications revolution, the idea of intelligent transportation systems, previously known as intelligent vehicle highway systems, began during the 1980s [1]. ITS can be defined as the application of advanced technologies to surface transportation problems, including traffic and transportation management, travel demand management, advanced public transportation management, electronic payment, commercial vehicle operations, emergency services management, and advanced vehicle control and safety systems. There are several promising uses of ITS, if implemented meticulously. ITS can be used to enhance mobility of vehicles, thus decreasing traveling times; to reduce fuel consumption and emissions, and instances of accidents caused by human error.

The promise of ITS has been recognized by organizations by creating avenues for research and implementation of ITS. For instance, the U.S. Department of Transportation (DOT) provides support for research and development, architecture and standards development, and field tests and model deployments in cooperation with the private sector [1, 2]. The European Union has also taken initiatives to promote research and development in ITS [3]. Similarly, in Asia and Australia, ITS have been implemented or proposed [4–6].

1.2 Automated Transportation System (ATS)

The concept of automated transportation system (ATS) has been extensively researched in the recent years, and in some cases they have been implemented on a test-basis [7]. In an ATS, a vehicle is guided down the roadway with little or no human intervention, combined with the sharing of traffic information and road conditions between vehicles and a smart roadside infrastructure. Efficient and secure implementation of ATS would be able

to optimize the usage of busy highways, and hence reduce traffic congestion; would make the need for manual control obsolete, and hence encourage people incapable of driving a vehicle to travel alone; would reduce emissions, fuel consumption, and injuries. In order to utilize these benefits in a secure manner, localization of vehicles in a ATS system becomes important.

There have been localization methods proposed for wireless sensor nodes. Distance bounding and verifiable multilateration are a few of the common localization methods which can be implemented in specific scenarios [8]. However, we must examine a secure localization method before using it for a specific scenario. A localization method can be prone to a number of attacks [9]. The distance bounding (DB) protocol, for instance, is prone to sybil attack wherein an adversary can make a legitimate node appear to be in a false location by stealing its identity and sending a response that causes a verifier to calculate false localization information [10]. In case of multiple verifiers, a number of adversaries can collude with each other to spoof a position for the legitimate vehicle. We examine which positions of a legitimate vehicle can be spoofed by an adversary or colluding adversaries in an infinite highway-line using solely DB and then using DB with trilateration.

1.3 Wireless Sensor Network (WSN)

Wireless sensor networks (WSNs) are larger scale networks of sensor nodes capable of sensing information from the environment, processing the sensed data, and transmitting it to the remote locations [11]. WSNs are mostly used in low bandwidth and delay tolerant applications. WSNs have several distinctive features such as unique network topology, diverse applications, unique traffic characteristics, and severe resource constraints.

Components of a WSN include one or more base stations or sink nodes connected to a large number of sensor nodes scattered in a physical space. The number of sensor nodes differ according to application and can extend upto several thousands in a given network. The sensor nodes can sense physical information, process crude information, and report them to the sink. The sink, in turn, queries the sensor nodes for information. A typical wireless sensor node consists of the following components: the sensor unit, the processing

unit, the transmission unit, and the unit of energy control. Depending on the area of application, it may also contain additional modules such as positioning system (e.g. GPS), or an energy generating system (e.g. solar cells) [12, 13].

1.4 Vehicular Ad-hoc Networks (VANETs)

Vehicular ad-hoc networks (VANETs) is a sub-category of ITS which are wireless communication networks that provide interesting roadside services such as vehicular safety, traffic congestion, alternate routes, estimated time to destination, and in general improves the efficiency and safety on the road. Each vehicle in VANETs is equipped with a wireless on-board unit (OBU) that allows the vehicle to communicate with other vehicles or with road side units (RSUs) through short-range wireless communication [14] . VANETs involve two modes of communications: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. VANETs use the dedicated short-range communications (DSRC) standard capable of communicating within a range of 1000 m at typical highway speeds. It provides seven 10 MHz channels at the 5.9 GHz licensed band for ITS applications, with different channels designated for different applications [15].

VANETs are advantageous as compared to long-range wireless communication through internet-based or cellular system-based services. Some of these advantages are: lower latency due to direct comuinication, broader coverage, and no service fee. The advantages of VANETs have elicited some research projects around the world, by governments (e.g. the vehicle safety communications consortium in USA [16] and car-to-car communications consortium in Europe [17]), academia (e.g. UCLA campus vehicular testbed and vehicular networking systems research laboratory at UM-Dearborn) and industry (e.g. Probabilistic routing for vehicular ad hoc network patented by Toyota [18] and European automobile companies, Audi, BMW, DaimlerChrysler, Fiat, Renault, and Volkswagen, formed a car-to-car communications consortium).

1.5 Challenges in Vehicular Ad-hoc Networks

There are certain challenges which need to be addressed in order to avail of the advantages of VANETs. They can be broadly categorized as follows [15, 19].

Authenticity/Integrity: VANET participants, OBU and RSU, need to check the authenticity and integrity of the received messages. This helps preventing sybil attacks and falsifying position information.

Privacy/Confidentiality: Privacy, on one hand, and the ability to trace the source of misbehaving vehicles, on the other hand, are two contradicting issues. In particular, the privacy preservation in VANETs should be conditional, where senders are anonymous to receivers while traceable by the authority. With traceability, the authority can reveal the sender's identity of a message once a dispute occurs.

Information availability: A vehicle's data should be available to all other vehicles around, all the time. This requirement may consume network resources.

Short-term linkability: For privacy, an eavesdropper should not be able to link messages from the same OBU in the long-term. However, some VANETs applications require that in the short-term, a recipient be able to link two messages sent out by the same OBU.

Traceability and revocation: An authority should be able to trace an OBU that abuses the system. Also, once a misbehaving OBU has been traced, the authority should be able to revoke it in a timely manner. This prevents the misbehaving OBU from causing any further damage.

Efficiency: OBUs must have resource-limited processors to make VANETs economically viable. Therefore, the cryptography used in VANETs should incur limited computational overhead.

Chapter 2

Background

In a wireless sensor network (WSN), such as a vehicular ad-hoc network (VANET), there are two types of sensor nodes involved during localization [9, 20].

Unknown node: The node whose position needs to be determined is called an unknown node.

Anchor node: The node whose position is known and which helps in the localization process is called an anchor node or beacon node.

Some of the localization methods have been discussed in the following sections.

2.1 Range-based Methods

In these type of methods, the range, i.e. the distance between the anchor node and unknown node, is determined and then using this distance information from different anchor nodes, the position of the unknown node is estimated. This is a fine-grained approach to localization as it attempts to measure the exact distance between the unknown and anchor node. Some popular methods of calculating the range are as follows.

2.1.1 Received Signal Strength Indicator (RSSI)

RSSI measures the power of the signal at the receiver [21]. Based on the known transmit power, the effective propagation loss can be computed. Since a measurement of signal strength provides a distance estimate between the transmitter and the reciever, the transmitter must lie on a circle centered at the receiver. The power level at the receiver is given by

$$P_r = P_t c_1 (\frac{c_2}{d})^n, \tag{2.1}$$

where P_t is the power level on which the message is sent and n, c_1, c_2 are constants related

to physical environment, the antenna gains, and carriers wavelength, respectively. Since, P_r and P_t can be measured, the distance d can be estimated from this formula. The method by Viani *et al.* uses RSSI data collected from test objects placed at known locations [22]. A Support Vector Machine (SVM) is trained to obtain the relationship between the test objects position at each time instant and the signals received by the anchor nodes (quantified by the RSSI). A system composed of N sensors located at positions $(x_n, y_n); n = 1, ..., N$ and an investigation domain of coordinates (x, y) is defined. The investigation domain is denoted by $I_D = \frac{-X_D}{2} \leq x \leq \frac{X_D}{2}$ and $\frac{Y_D}{2} \leq y \leq \frac{Y_D}{2}$. The domain, I_D is partitioned into a 2-dimensional lattice of C squared cells centered at (x_c, y_c), $c = 1, ..., C$. The localization problem is recast as the probability of the presence of an object in each cell starting from the knowledge of the RSSI values of the whole set of $N \times (N - 1)$ node links. The problem solution is the computation of the posteriori probability[1] distribution at each time-instant. An RSSI-based scheme can be obtained for VANETs using dedicated short-range-communication (DSRC) protocol which uses the IEEE 802.11p standard to support low-latency vehicle-to-vehicle and vehicle-to-infrastructure communications [23, 24]. The drawback of using RSSI is that there are factors such as multipath fading, shadowing and non-line-of-sight errors which need to be taken into account [25]. Also, the distance measurements can be noisy due to limitations of the hardware. Mobility complicates the handling of noise, and in noisy environments, measurements can be misconstrued as observed motion. Also, for vehicular networks, this method may not be feasible because the effects of fading becomes prevalent when mobility increases.

2.1.2 Time of Arrival (ToA) and Time Difference of Arrival (TDoA)

These are time-based methods which use the propagation-time of a signal to determine the distance between nodes. The propagation-time can be directly translated into distance, based on known signal propagation speed. If the signal propagates in time t from the target transmitter to the receiver, then the receiver is at the range R given by $R = c.t$, where c

[1]Posteriori probability distribution is the distribution of an unknown quantity treated as a random variable, conditional on the evidence obtained from an experiment or survey.

is the speed of light. TOA allows the receiver node to know the distance of itself from the transmitter node. If we use multiple receiver nodes, TDoA allows the system to determine relative position of the transmitter node from the multiple receiver nodes by examining the difference in time at which the signal arrives at each receiver node. Distance bounding is a popular method that estimates distance based on ToA. We will discuss this approach in details in the later sections of this chapter. The time-of-ight-based methods determine distances by measuring the propagation delay of a signal, we require high-resolution time measurements, accurate real-time clock synchronization between nodes, and line-of-sight-propagation conditions. To keep an accurate real-time clock synchronization among mobile nodes becomes diificult. Research has been done to make it more robust for mobile nodes [26, 27].

2.1.3 Angle of Arrival (AoA)

Angle of Arrival techniques estimate the desired target by measuring the angle at which signals from several transmitters arrive at the receiver through the use of directive antennas or antenna arrays [28, 29]. AoA techniques may introduce errors by multipath fading and shadowing, the non-line-of-sight (NLOS) propagation and multiple-access interference. Researchers are attempting to make this method more accurate by eliminating errors caused by multipath propagation [30, 31].

2.2 Range-free Methods

The range-free methods do not try to measure parameters that will enable them to exactly calculate distances between nodes. They try to estimate the distance between nodes using data based on network connectivity and map reading. Some of the methods that follow this approach are MDS map, DV hop, SLAM, and cooperative localization methods.

2.2.1 Multi-dimensional Scaling (MDS) Map

It determines the positions of nodes when a node is given only basic information (e.g. a

node may be given information of the nodes which are within communication range of the given node). If the distances between neighboring nodes can be measured, that information can be easily incorporated into the method. MDS map is able to generate relative maps that represent the relative positions of unknown nodes when there are no anchor nodes that have known absolute coordinates. When the positions of a sufcient number of anchor nodes are known, e.g. three anchors for 2-dimensional localization and four anchors for 3-dimensional, MDS map then determines the absolute coordinates of all nodes in the network [32]. MDS map has three steps.

Step I: Use an all-pairs shortest-paths algorithm to roughly estimate the distance between each pair of unknown nodes with the available network connectivity information in the beginning.

Step II: Use multi-dimensional scaling (MDS), a technique from mathematical psychology, to derive node locations that fit those estimated distances.

Step III: Normalize the resulting coordinates to take into account any nodes whose positions are known [33].

The network is represented as an undirected graph with vertices and edges. The vertices correspond to the anchor nodes. The localization is based on two methods.

Proximity-only: A node only has information about which nodes are its neighbors, by means of some local communication channel such as radio or sound. But, a node does not know how far away these neighbors are or in what direction they lie. Here the edges in the graph correspond to the connectivity information with neighbouring nodes.

Proximity and distance: The proximity information is enhanced by knowledge of the distances, between neighboring nodes. Here the edges are associated with values corresponding to the estimated distances. MDS map is advantageous if the number of anchor nodes in the network are low. Even with low number of anchor nodes, MDS map is able to localize the unknown nodes. However, MDS map does not work well on irregularly-shaped networks as the inter-node distances vary to a large extent and hence the estimated inter-node distance and the actual distance between two-nodes may have a large error.

2.2.2 Distance Vector (DV) Hop

This method assumes a heterogeneous network consisting of sensing and anchor nodes. The anchor nodes flood their location throughout the network. When they cross a node along the way, they increment a running hop-count. Unknown nodes calculate their position based on the received anchor node locations, the hop-count from the corresponding anchor node, and the average-distance per hop which is obtained through anchor to anchor communication. The DV hop algorithm by Niculescu and Nath uses a distance vector exchange such that the distances between nodes and landmarks are expressed in terms of hops [34]. Each node maintains a table $[X_i; Y_i; h_i]$ and exchanges updates only with its neighbors. Once a landmark gets distances to other landmarks, it estimates an average size for one hop, which is then deployed as a correction to the entire network. An arbitrary node after a correction may then have estimate distances to landmarks, in meters, which can be used to perform triangulation [35].

2.2.3 Simultaneous Localization and Mapping (SLAM)

The localization problem of SLAM is posed in the following manner. "Is it possible for an autonomous vehicle to start in an unknown location in an unknown environment and then to incrementally build a map of this environment while simultaneously using this map to compute absolute vehicle location [36]?" The autonomous vehicle which needs to be localized first collects data using sensors, RADAR [37], GPS [37], or using methods like dead-reckoning [38]. It then builds a map of the surrounding objects, and as more data is received, the node optimizes its map using techniques like Kalman filters [39, 40].

2.2.4 Cooperative Localization

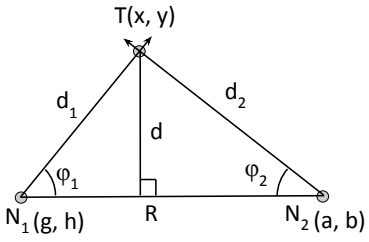
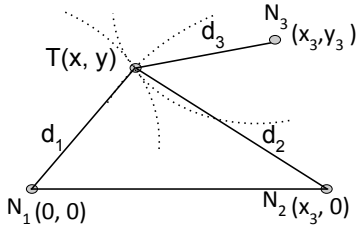
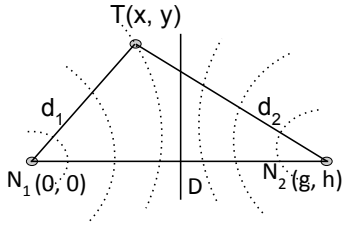
The cooperative localization techniques depend on the knowledge of surrounding nodes to relatively localize a node with respect to it's neighbours. This method relies on algorithms based on the principles of estimation theory and statistical inference [41–43]. These techniques are useful when a node is not able to communicate with the verification infrastructure. By utilizing the localization knowledge of other nodes, a given node can have

an acceptable estimation of its own location within the network. Sometimes cooperative localization is used in conjunction with a range-based method as as time difference of arrival or angle of arrival [28, 29].

2.3 Geometric Methods

The range-based methods depend on geometric methods for the position determination aspect of localization. Hence, we analyze some of the popular geometric methods of localization. After the anchor nodes estimate the distance of an unknown node from each of them, they cooperatively localize the unknown node using their distance information. Table 2.1 depicts how this can be done using three popular geometric methods, namely, triangulation, multilateration, and hyperbolic principle [14].

Table 2.1: Summary of the three geometric methods of localization.

Basic Approach	Figure
Triangulation: – Angles of two sides, Φ_1 and Φ_2 are calculated to get desired location when the distance point is unknown – Importantly the desired point has to be intersection of two lines from two sides	
Multilateration: – An extension of Triangulation with three reference points – Three point of intersection will give calculated distance value from reference point to object T.	
Hyperbolic principle: – It is a set of points that have constant difference values from two fixed points Hyperbola's focus is represented by each point where focus is an anchor node or reference point – Position can be calculated when the target resides between two foci of hyperbola curve – Curve's distance to each hyperbola focus are fixed	

2.3.1 Triangulation

Consider the diagram for triangulation in Table 2.1. At the point of intersection, T, the anchor nodes, N_1 and N_2, subtend angles, Φ_1 and Φ_2, respectively. The distance between N_1 and N_2 is given by

$$R = \frac{d}{\tan \Phi_1} + \frac{d}{\tan \Phi_2}, \tag{2.2}$$

where d is the perpendicular distance of T from the line joining N_1 and N_2. The value of d can be calculated by using the following formula.

$$d = \frac{R \sin \Phi_1 \sin \Phi_2}{\sin \Phi_1 + \sin \Phi_2}, \tag{2.3}$$

where

$$\Phi_1 = \tan^{-1} \frac{h - Y}{g - X}, \tag{2.4}$$

$$\Phi_2 = \tan^{-1} \frac{b - Y}{a - X}. \tag{2.5}$$

If we know the coordinates of the anchor nodes ((a, b) and (g, h)) in the figure, then we can find the coordinates of the unknown node, (X, Y).

$$X = \frac{b - h - a \tan \Phi_2 + g \tan \Phi_1}{\tan \Phi_1 - \tan \Phi_2}, \tag{2.6}$$

$$Y = x \tan \Phi_2 + (b - a \tan \Phi_1). \tag{2.7}$$

We can also find the respective distances, d_1 and d_2, between the anchor nodes, N_1 and N_2, and target point, T.

$$d_1 = |g - X| = \sqrt{(g - X)^2 - (h - Y)^2}, \tag{2.8}$$

$$d_2 = |a - X| = \sqrt{(a - X)^2 - (b - Y)^2}. \tag{2.9}$$

2.3.2 Multilateration

The example in Table 2.1 shows multilateration with three anchor nodes. The distances

from each node is determined using a time difference of arrival protocol such as distance bounding. The unknown node lies anywhere along the circle with radius d_1 from N_1, d_2 from N_2, and d_3 from N_3. By solving the equations of these circles we determine the coordinates of the point of intersection of these three circles. These coordinates are in fact, the location of the unknown node. The distances from N_1, N_2, and d_3, respectively, are as follows.

$$d_1 = (t_1 - t_0)c, \tag{2.10}$$

$$d_2 = (t_2 - t_0)c, \tag{2.11}$$

$$d_3 = (t_3 - t_0)c, \tag{2.12}$$

where t_0 is time at which a signal was sent from T to the three anchor nodes, d_1 is distance between N_1 and T, t_1 is the time of arrival of signal T to N_1, t_2 is the time of arrival of signal T to N_2, t_3 is the time of arrival of signal T to N_3. The equations of the three intersecting circles are given by

$$d_1^2 = X^2 + Y^2, \tag{2.13}$$

$$d_2^2 = (X - x_2)^2 + Y^2, \tag{2.14}$$

$$d_3^2 = (X - x_3)^2 + (Y - y_3)^2. \tag{2.15}$$

The coordinates of the unknown node obtained by solving these three equations are

$$X = \frac{x_2^2 + d_1^2 - d_2^2}{2x_2}, \tag{2.16}$$

$$Y = \frac{x_3^2 + y_3^2 - d_1^2 - d_3^2 - 2Xx_3}{2y_3}. \tag{2.17}$$

2.3.3 Hyperbolic Principle

In this method, the two cooperating anchor nodes, N_1 and N_2, can calculate a path difference, Δd from a given transmitter in Table 2.1. This path difference corresponds to the equation of a hyperbola. And by solving this equation for X and Y, we can get the

coordinates of the unknown node.

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1, \tag{2.18}$$

where a and b can be obtained from the quantities Δd and D in Table 2.1.

$$a^2 = (\frac{\Delta d}{2})^2, \tag{2.19}$$

$$b^2 = (\frac{D}{2})^2 - a. \tag{2.20}$$

The path difference Δd can be calculated either using the time-delay of recieved signal (similar to multilateration) or using a path-loss model such as the log-normal shadowing model [44] as given by equation (2.21).

$$L(d) = L(d_0) + 10\eta \log(\frac{d}{d_0}) + X_\sigma. \tag{2.21}$$

Here, d_0 is a predened reference distance close to the transmitter, $L(d_0)$ is the average path loss at the reference distance, and η is a path loss exponent dependent upon the propagation environment. The signal shadowing is represented by a random variable X_σ with zero mean and standard deviation σ. Table 2.2 summarizes the localization techniques we have discussed. For automated vehicles travelling along a dedicated highway, precision of location is necessary. Therefore, we use a fine-grained approach based on ToA. This algorithm is known as distance bounding. For determining the position we analyse the geometric method of trilateration, which is a case of multilateration with three anchor nodes. In the subsequent sections, we introduce the distance bounding algorithm and the technique called verifiable trilateration.

2.4 Distance Bounding (DB)

Distance bounding is a method which enables a verifier to establish an upper bound on the physical distance to a prover. Distance bounding is based on timing the delay between

Table 2.2: Localization techniques and their features.

Range-based	Range-free
Examples: RSSI, ToA/TDoA, AoA	Examples: MDS map, DV hop, SLAM
These methods require complex hardware.	The hardware depends on the type of sensors used.
Some methods need time-synchronization between the transmitter and receiver.	No time synchronization is required.
They follow a fine grained approach.	They follow a coarse grained approach.
These methods are affected by errors due to multipath fading, shadowing and NLOS.	These methods are not affected by errors due to signal propagation.
They are ideal for non-uniformly distributed networks.	They are ideal for uniformly distributed networks.
The network requires sufficiently large number of anchor nodes.	The network can localize with less number of anchor nodes.
Localization requires coordinates of only a minimum number of nodes.	Locaization requires the coordinates or hop-information of a large number of nodes.

sending out a challenge bits and receiving back the corresponding response bits. The delay time for responses enables the verifier to compute an upper-bound on the distance, as the round trip delay time divided into twice the speed of light [8, 45, 46]. The computation is based on the fact that electromagnetic waves travel nearly at the speed of light in free space but cannot travel faster. Since, the speed of light remains constant, the only factor that can influence the distance estimation is the time delay. The verifier stations assume a known time delay to process the challenge bits and generate the response bits. The actual distance of a vehicle from a verifier cannot be reduced (as the propagation time cannot be reduced). But, it can be increased (by deliberately introducing a time delay) so that the estimated distance of a vehicle is larger than its actual distance. A malicious vehicle can therefore position itself along the highway in such a way that it can spoof any location whose distance is larger from the verifier station than itself.

We perform our analysis based on the distance bounding protocol by Brands and

Chaum [47]. The protocol is based on a prover (P), trying to authenticate itself to a verifier (V), whose task is to establish an upper-bound on the prover's distance from itself. The prover starts a series of rapid bit exchanges with a security parameter, k. Before these bit exchanges take place, a random bit string of length k ($m_1.....m_k$) is already sent by the verifier, V to the prover, P. The following steps are implemented after P receives the message, $m_1.....m_k$.

Step I: V generates uniformly, at random k bits for a rapid bit exchange, N_i where $i = 1$ to k.

Step II: A series of bits of challenges and responses are exchanged quickly. P responds as soon as possible bit by bit with a series of n bits $f(N_i)$ to the corresponding bits received from verifier, N_i. The response of the prover is calculated by P performing an exclusive OR between the bit N_i and the received bit m_i.

Step III: The prover, P, calculates a sign bit string x by concatenating pairs of N_i and $f(N_i)$ bits to create a series of bits which are then transmitted to V. The calculated x by V is compared to the x received by V. If the received signature is correct, V computes the maximum distance at which P is located, using the Round-Trip Time (RTT) of bits exchanged during *Step II*, using the speed of an electromagnetic wave.

According to Brands and Chaum, since, today's electronics can manage computation times upto a few nanoseconds, and light can travel about 30 cms in a nanosecond, the error caused due to delay in device processing is much less [47]. Hence, distance bounding can be an efficient protocol for localization. We will apply distance bounding to our specific case of localization of a point on an infinite highway.

Protocol 2.1 The basic Brands and Chaum distance bounding protocol.

$i =$	$0, 1, 2, ..., k$
$V \rightarrow P$:	N_i at $t = t_{si}$
$P \rightarrow V$:	$f(N_i)$ at $t = t_{ri}$
V :	**Calculates** $f(N_i^n)$
If received bits =	calculated bits,
V :	**Calculates** $RTT = t_s - t_r + T_p$ and $DB = \frac{c(RTT - T_p)}{2}$

2.5 Verifiable Trilateration

We know the geometric method of multilateration. Verifiable multilateration (VM) is a mechanism that enables location verification in wireless sensor networks with the help of simultaneous working verifiers. This mechanism relies on authenticated ranging or distance bounding within a verification triangle (triangular pyramid) formed by the location verifiers. Due to the property of the distance bounding protocol, attackers can only enlarge (but not reduce) the measured distance between the infrastructure and the node. Therefore, if multiple verifiers work simultaneously, we can locate a point in space. Figure 2.1 gives a schematic diagram of how a point in 2-dimensional space can be located by three verifiers using the distance bounding protocol. When we use three verifiers, the method is called verifiable trilateration. According to Capkun and Hubaux, the intuition behind the verifiable multilateration algorithm is the following [8].

> "Because of the distance bounding property, the claimant can only pretend to be more distant from the verifier than it really is. If it increases the measured distance to one of the verifiers in order to keep the position consistent, the claimant needs to prove that at least one of the measured distances to other verifiers is shorter than it actually is, which it cannot because of distance bounding."

This can be explained with a simple example: if an object is located within the triangle and it moves to a different position within the triangle, it will certainly reduce its distance to at least one of the triangle vertices [48]. The same properties hold if an external attacker enlarges distances between verifiers and an honest claimant. Protocol 2.2 gives the verifiable multilateration protocol using three verifiers.

2.6 List of Probability Distributions

We use certain probability distribution functions during our analysis of secure localization methods. These probability distributions are briefly reviewed in this section.

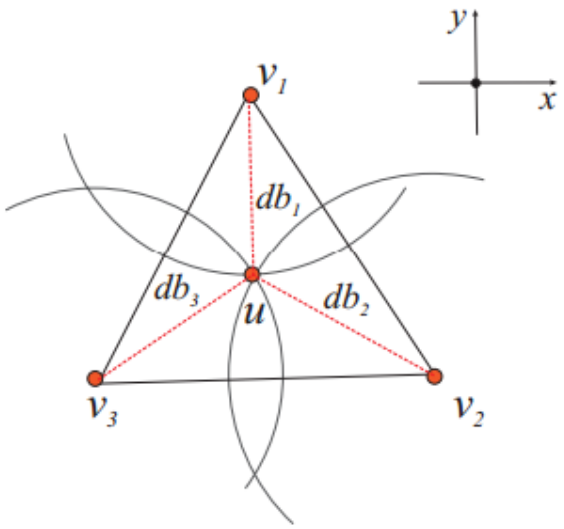


Fig. 2.1: Verifiable multilateration with three verifiers.

Protocol 2.2 The verifiable multilateration protocol.

$\tau = \Phi$; set of verifiers that form triangles around υ
$\nu = v_1, ..., v_n$; set of verifiers in the power range of υ
For all $v_i \in \nu$, perform distance bounding from v_i to υ and obtain db_i.
For all triplets $(v_i, v_j, v_k) \in \mu^3$,compute the position (x'_u, y'_u) with db_i, db_j, db_k by mean square error estimation.
If (x'_u, y'_u) in $\Delta(v_i, v_j, v_k)$ then $\tau = \tau \cup v_i, v_j, v_k$
With all $v_i \in \tau$, compute the position $(x"_u, y"_u)$ by mean square error estmation.
If for all $v_i \in \tau$, $\left| db_i - \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2} \right| \leq \delta$,
$x_u = x'_u$, $y_u = y'_u$
else the position is rejected.

2.6.1 Bernoulli Distribution

It is a discrete probability distribution defined for a Bernoulli trial which yields a success with probability p and failure with probability q such that $p = 1 - q$. For a random variable, X following Bernoulli distribution, the probability mass function is given by

$$f(x) = p^x (1-p)^{1-x} \quad x \in \{0, 1\}. \tag{2.22}$$

The mean or expected value is given by

$$E(x) = p. \tag{2.23}$$

And the variance, which is the square of the standard deviation (σ), is given by

$$\sigma^2(x) = p(1-p). \tag{2.24}$$

2.6.2 Binomial Distribution

It is a discrete probability distribution of the number of successes in a sequence of n independent Bernoulli trials, each of which yields success with probability p and failure with probability q where $p = 1 - q$. Bernoulli distribution is a special case of the binomial distribution when $n = 1$. For a random variable, X, following the binomial distribution with parameters n and p, we write $X \sim B(n, p)$. The probability mass function of getting exactly x successes in n trials is

$$f(x) = C_x^n p^x (1-p)^{n-x} \quad x \in \{0, 1, 2, ..., n\}, \tag{2.25}$$

where $C_x^n = \frac{n!}{x!(n-x)!}$. The mean or expected value is given by

$$E(x) = np. \tag{2.26}$$

And the variance, which is the square of the standard deviation (σ), is given by

$$\sigma^2(x) = np(1-p). \tag{2.27}$$

The probability mass function is given by

$$f(x) = p^x (1-p)^{1-x} \quad x \in \{0, 1\}. \tag{2.28}$$

The mean or expected value is given by

$$E(x) = p. \tag{2.29}$$

And the variance, which is the square of the standard deviation (σ), is given by

$$\sigma^2(x) = p(1-p). \tag{2.30}$$

2.6.3 Poisson Binomial Distribution

It is the discrete probability distribution of a sum of n independent Bernoulli trials that are not necessarily identically distributed[2]. For each of the n experiments, success probability is p_i and failure probability is q_i, where $p_i = 1 - q_i$ and $i \in 0, 1, 2, ..., n$. The ordinary Binomial distribution is a special case of the Poisson Binomial distribution, when all success probabilities are the same. For a random variable X following the binomial distribution with parameters n, p_i, and p_j where $i, j \in 0, 1, 2, ..., n$, the probability mass function of getting exactly x successes in n trials is

$$f(x) = \sum_{S \in F_x} \prod_{i \in S} (p_i) \prod_{j \in S^c} (1 - p_j) \;\; x \in \{0, 1, 2, ..., n\}, \tag{2.31}$$

where $S :=$ set of trials which were a success;

$S^c :=$ set of trials which were a failure;

$F_x :=$ set of subsets of x integers chosen from $0, 1, 2, ..., n$.

The mean or expected value is given by

$$E(x) = \sum_{i=1}^{n} p_i. \tag{2.32}$$

And the variance, which is the square of the standard deviation (σ), is given by

$$\sigma^2(x) = \sum_{i=1}^{n} p_i (1 - p_i). \tag{2.33}$$

2.6.4 Beta Distribution

It is a family of continuous probability distributions defined on the interval $[0, 1]$

[2] A sequence or other collection of random variables is independent and identically distributed if each random variable has the same probability distribution as the others and all are mutually independent.

parametrized by two positive shape parameters, denoted by α and β, that appear as exponents of the random variable and control the shape of the distribution. The probability density function of the beta distribution, for $0 \leq x \leq 1$, and shape parameters $\alpha > 0$ and $\beta > 0$ is

$$f(x) = \frac{x^{\alpha-1}\left(1-x^{\beta-1}\right)}{B(\alpha,\beta)}, \tag{2.34}$$

where $B(\alpha,\beta)$ is a normalizing constant.[3] $B(\alpha,\beta)$ is multiplied to the function such that its integration from $x = 0$ to $x = 1$ is unity. It is given by

$$B(\alpha,\beta) = \int_0^1 u^{\alpha-1}\left(1-u^{\beta-1}\right) du. \tag{2.35}$$

The mean or expected value is given by

$$E(x) = \frac{\alpha}{\alpha+\beta}. \tag{2.36}$$

And the variance, which is the square of the standard deviation (σ), is given by

$$\sigma^2(x) = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}. \tag{2.37}$$

[3] A normalizing constant is a constant by which a non-negative function must be multiplied so that the area under its graph is 1, to make it a probability density function or a probability mass function.

Chapter 3

Distance Bounding and Trilateration for Localization in an Automated Transportation System

We discussed localization for vehicular ad-hoc networks (VANETs), which is a subcategory of intelligent transportation systems (ITS). In this chapter, we apply the methods of distance bounding and trilateration for an automated transportation system (ATS). We describe a distance bounding and trilateration infrastructure and describe threat models for each of the infrastructures. In the end, we schematically illustrate the different attack scenarios that are possible in these infrastructures.

3.1 Definitions

We refer to an anchor node as a verifier and the vehicle whose location is to be determined as a prover. In order to make our analysis easier, we define a few terms vis-a-vis an ATS infrastructure. We will use these terms in the subsequent sections.

Definition 1 *Verifier range*: The maximum distance over which a verifier is able to send a signal of acceptable quality.

Definition 2 *Verifier scope*: The length of the segment of the highway such that a verifier is responsible for the localization of a vehicle lying on any point belonging to that segment.

Definition 3 *Verification unit*: The basic unit of the highway infrastructure consisting of the minimum number of verifiers needed to localize a vehicle on the highway and the segment of the highway for which this number of verifiers can be considered a standalone highway infrastructure.

Definition 4 *Verification segment*: For a given verification unit, the segment of the highway such that the responsibility of localization of a point on it is assigned to that verification unit.

Definition 5 *Spoofing range*: The length of the largest segment on the highway such that an attacker can spoof the position of a given vehicle from any point on that segment by beguiling a given verifier.

Definition 6 *Jamming range*: The maximum verifier range under the effect of a benign jammer intended to restrict communication between a verifier and a vehicle for security purposes.

Definition 7 *Effective vehicle length*: The length on the highway required to accommodate a single vehicle. It is the sum of the length of the vehicle and the mandatory separation distance that need to be maintained between consecutive vehicles on the highway.

Definition 8 *Vehicle position*: The point on the highway on which the leading edge of a vehicle lies. Since, localization is in terms of the position of a point, we will consider the leading edge of a vehicle to be its position on the highway.

3.2 Threat Model for Distance Bounding and Trilateration

The threat model describes the attacker's goals and capabilities for a given infrastructure. In our analysis we consider two colluding attackers in the system who possess the identity of one or more legitimate vehicles in the system. The attackers are capable of sharing and using these identities as required. The goal of the attackers is to use the identity of a legitimate vehicle to falsely localize (spoof) that vehicle on the targeted vehicle position. The attackers and the target vehicle travel along the same lane on the highway and hence cannot overtake each other. Also, the attackers do not have control over their initial position on the highway. For a given vehicle position, the attackers can lie anywhere on the highway. We now, define the following infrastructures and analyze them according to our threat model.

3.3 Infrastructure Implementing Distance Bounding and Trilateration

3.3.1 Distance Bounding with Two Verifiers

Consider an infrastructure consisting of verifiers fixed along an infinite highway. Each verifier uses the distance bounding algorithm to determine an upper bound to distance of a prover. Let there be m number of verifiers in a verification unit. Then, the corresponding distance bounding algorithm is given by Protocol 3.1. We observe that this algorthm is for a generic infrastructure which uses m verifiers every time a prover position needs to be determined. We will use this algorithm for $m = 2$ (implementing only distance bounding) and $m = 3$ (implementing trilateration with the distance bounding algorithm). For the infrastructure with $m = 2$, we assume an infinite highway with verifiers placed on the highway as shown in Figure 3.1. There are two verifiers involved in each verification unit. For instance, the verifiers, V_1 and V_2, form a verification unit as they work simultaneously to estimate the position, P, of a prover vehicle travelling between them. V_1 determines a upper-bound on the distance of P from itself. So P cannot lie further along the highway, than this distance. Similarly, V_2 also determines a upper-bound on how far P can be from itself. From these estimated bounds the position of P between V_1 and V_2 can be estimated.

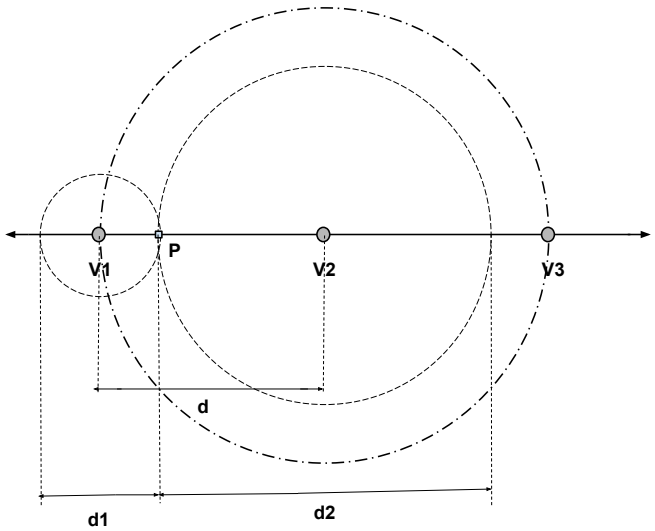


Fig. 3.1: Distance bounding infrastructure: verifier range = d, verifier scope = 2d; In case of a vehicle at position, P: verification unit = V_1, V_2; verification segment = V_1 to V_2; spoofing range of $V_1 = d_1$; spoofing range of $V_2 = d_2$.

Protocol 3.1 Verifying a vehicle's location using distance bounding with m number of verifiers in a verification unit.

$i =$	$0, 1, 2, ..., k$
$v =$	verifier number
$m =$	number of verifiers in a verification unit
At $t = t_{si}$	
$V_n \rightarrow P:$	N_i^n
$V_{n+1} \rightarrow P:$	N_i^{n+1}
$V_{n+2} \rightarrow P:$	N_i^{n+2}
	.
	.
	.
$V_{n+(m-1)} \rightarrow P:$	$N_i^{n+(m-1)}$
At $t = t_{ri}$	
$P \rightarrow V_n:$	$f(N_i^n)$
$P \rightarrow V_{n+1}:$	$f(N_i^{n+1})$
$P \rightarrow V_{n+2}:$	$f(N_i^{n+2})$
	.
	.
	.
$P \rightarrow V_{n+(m-1)}:$	$f(N_i^{n+(m-1)})$
$V_n:$	**Calculates** $f(N_i^n)$
$V_{n+1}:$	**Calculates** $f(N_i^{n+1})$
$V_{n+2}:$	**Calculates** $f(N_i^{n+2})$
	.
	.
	.
$V_{n+(m-1)}:$	**Calculates** $f(N_i^{n+(m-1)})$
If received bits =	calculated bits,
$V_n:$	**Calculates** $RTT_n = t_s n - t_r n + T_p$
	$DB_n = \frac{c(RTT_n - T_p)}{2}$
$V_{n+1}:$	**Calculates** $RTT_{n+1} = t_{s(n+1)} - t_{r(n+1)} + T_p$
	$DB_{n+1} = \frac{c(RTT_{n+1} - T_p)}{2}$
$V_{n+2}:$	**Calculates** $RTT_{n+2} = t_{s(n+2)} - t_{r(n+2)} + T_p$
	$DB_{n+2} = \frac{c(RTT_{n+2} - T_p)}{2}$
	.
	.
	.
$V_{n+(m-1)}:$	**Calculates** $RTT_{n+(m-1)} = t_{sn+(m-1)} - t_{rn+(m-1)} + T_p$
	$DB_{n+(m-1)} = \frac{c(RTT_{n+(m-1)} - T_p)}{2}$

Here, we assume $m = 2$. Therefore, by using the above protocol we have the algorithm given by Protocol 3.2.

Protocol 3.2 Verifying a vehicle's location using distance bounding with two verifiers in a verification unit (basic distance bounding implementation).

$i =$	$0, 1, 2, ..., k$
$v =$	verifier number
$m =$	number of verifiers in a verification unit
At $t = t_{si}$	
$V_n \rightarrow P:$	N_i^n
$V_{n+1} \rightarrow P:$	N_i^{n+1}
At $t = t_{ri}$	
$P \rightarrow V_n:$	$f(N_i^n)$
$P \rightarrow V_{n+1}:$	$f(N_i^{n+1})$
$V_n:$	**Calculates** $f(N_i^n)$
$V_{n+1}:$	**Calculates** $f(N_i^{n+1})$
If received bits =	calculated bits,
$V_n:$	**Calculates** $RTT_n = t_s n - t_r n + T_p$
	$DB_n = \frac{c(RTT_n - T_p)}{2}$
$V_{n+1}:$	**Calculates** $RTT_{n+1} = t_s n + 1 - t_r n + 1 + T_p$
	$DB_{n+1} = \frac{c(RTT_{n+1} - T_p)}{2}$

3.3.2 Vulnerability Analysis of Distance Bounding with Two Verifiers

It requires a minimum of two attackers to defeat this method. If two malicious vehicles on the same or adjacent verification segment have the location information of a target vehicle, they can impersonate this vehicle and generate false position information. As the attackers move from one verification unit to another, we have three different scenarios of spoofing. Figures 3.2, 3.3, and 3.4 depict the three best case scenarios for two attackers, A_1 and A_2, to spoof the position of any vehicle lying on the highway-segment of length d by simultaneously beguiling the verifiers involved in that verification unit.

In the first attack scenario, shown in Figure 3.2, A_2 is in the verification unit V_1,V_2 and is approaching V_2, V_3 while A_1 is already in V_2, V_3. The attackers can spoof any point on the segment of length, d by beguiling V_2 and V_3. A_2 is closer to verifier, V_2 while A_1 is closer to V_3. Therefore, in order to spoof a position between V_2 and V_3, A_2, and A_1 must simultaneously beguile V_2 and V_3, respectively. A_2 can spoof any position on the segments labeled as A_2V_2 by beguiling V_2. Similarly, A_1 can spoof any position on the segments labeled as A_1V_3 by beguiling V_3. Any point on the segment of length d can be effectively spoofed by A_1 and A_2. Figures 3.3 and 3.4 depict the other two scenarios.

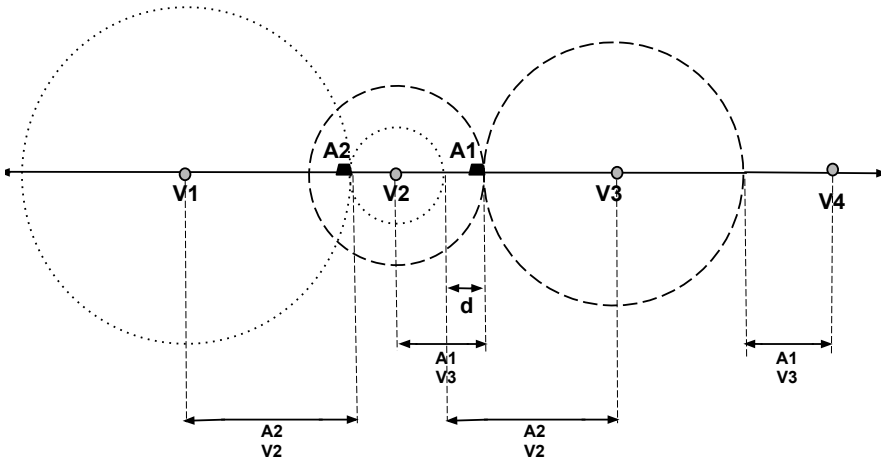


Fig. 3.2: Distance bounding, attack scenario I: The attackers (A_1 and A_2) are in adjacent verification units.

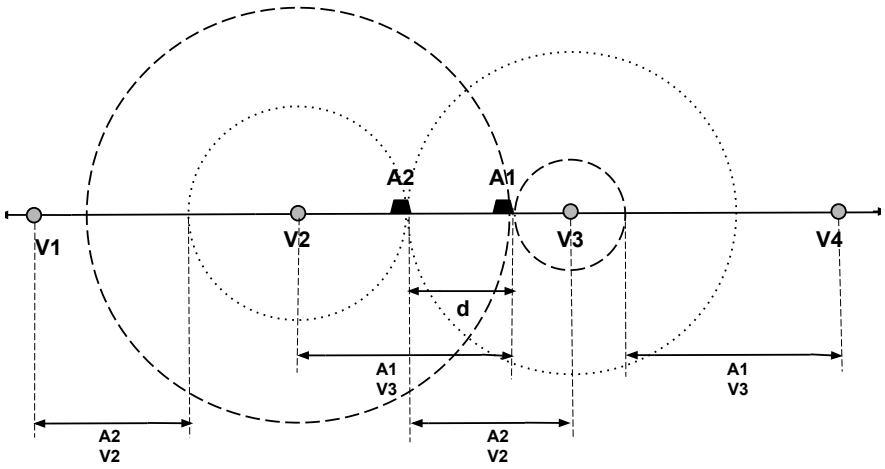


Fig. 3.3: Distance bounding, attack scenario II: Both the attackers lie in the same verification unit (V_2,V_3).

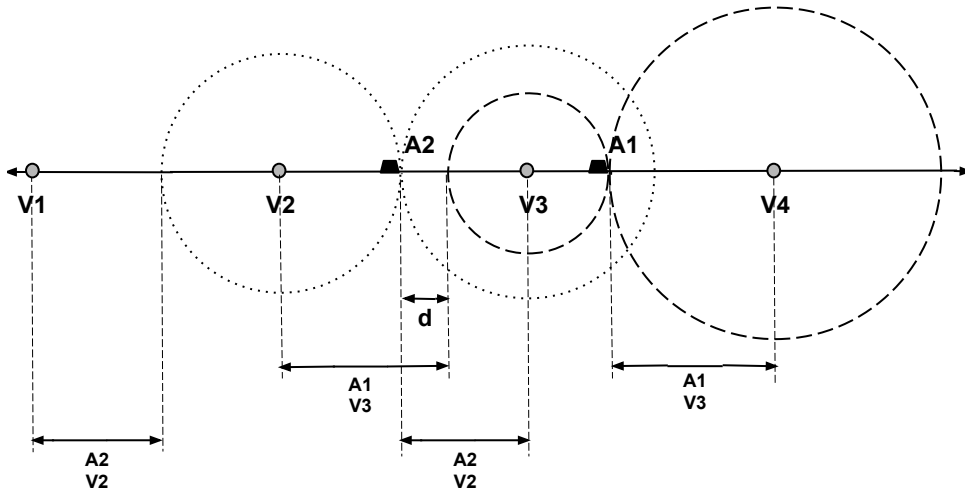


Fig. 3.4: Distance bounding, attack scenario III: A_1 has crossed the former verification unit and entered a new one (V_3, V_4). However, A_1 is still closer to V_3 as compared to A_2.

3.3.3 Distance Bounding with Three Verifiers (Trilateration)

The assumed architecture consists of individual vehicles or vehicle platoons moving on an infinite highway which runs through a series of triangles formed by verifiers placed along the highway. There are three verifiers acting simultaneously to locate a vehicle on the highway. One verifier forms the vertex of three different triangles. Each verifier is responsible for verification of vehicles within the triangles whose vertex it forms. This infrastructure is shown in Figure 3.5.

We notice that changing the perpendicular distance of a verifier from the highway does not affect the verifier scope or the spoofing range. Figure 3.6 illustrates this with three different infrastructures. The lines connecting the verifiers intersect on the highway at the same points (P_1 to P_6). Also, the circles determining the position P for each architecture type intersect at the same points on the highway. These points of intersection demarcate the segments which can be spoofed from behind and the front of a vehicle at position P.

Three verifiers, V_1, V_2, and V_3, use the distance bounding protocol simultaneously to find an upper-bound of the distance of a prover P from each of them and estimate a position on the highway according to Protocol 3.3.

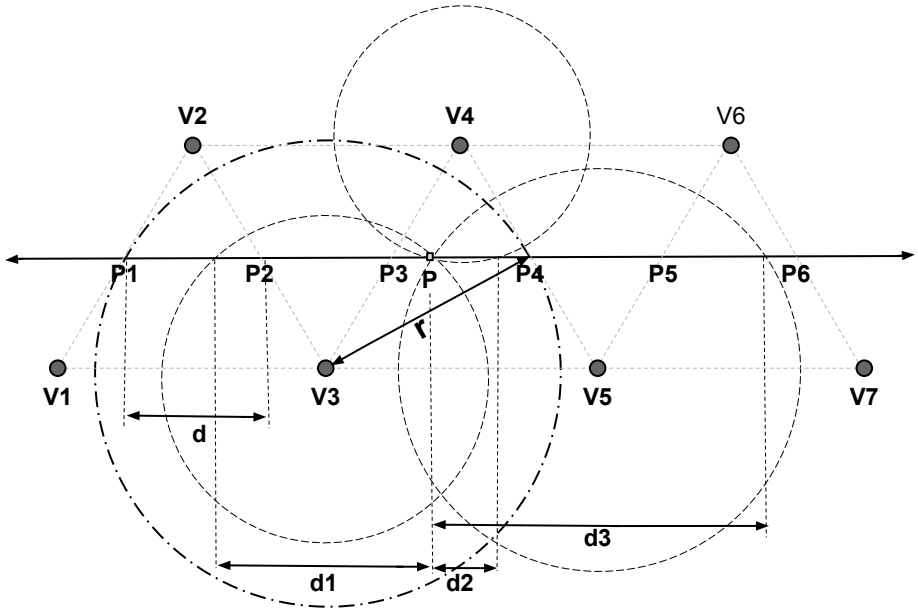


Fig. 3.5: Trilateration infrastructure: verifier range = r, verifier scope = 3d. In case of a vehicle at position, P: verification unit = V_3, V_4, V_5; verification segment = P_3 to P_4; spoofing range of $V_3 = d_1$; spoofing range of $V_4 = d_2$; spoofing range of $V_5 = d_3$.

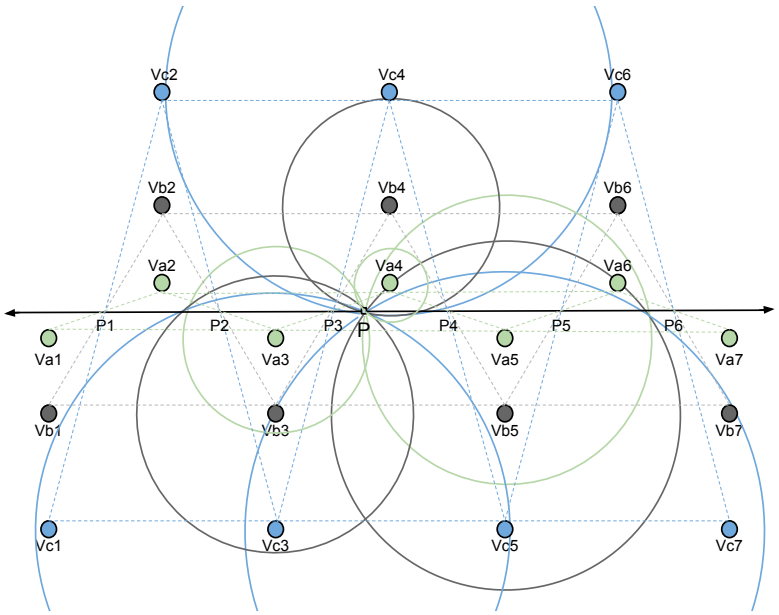


Fig. 3.6: Trilateration infrastructures (a, b, and c) consisting of five verification units and with the respective verifiers marked as V_{an}, V_{bn}, and V_{cn}; $n = 1$ to 7.

Protocol 3.3 Verifying a vehicle's location using distance bounding with three verifiers in a verification unit (trilateration).

$i =$	$0, 1, 2, ..., k$
$v =$	verifier number
$m =$	number of verifiers in a verification unit
At $t = t_{si}$	
$V_n \rightarrow P:$	N_i^n
$V_{n+1} \rightarrow P:$	N_i^{n+1}
$V_{n+2} \rightarrow P:$	N_i^{n+1}
At $t = t_{ri}$	
$P \rightarrow V_n:$	$f(N_i^n)$
$P \rightarrow V_{n+1}:$	$f(N_i^{n+1})$
$P \rightarrow V_{n+2}:$	$f(N_i^{n+2})$
$V_n:$	**Calculates** $f(N_i^n)$
$V_{n+1}:$	**Calculates** $f(N_i^{n+1})$
$V_{n+2}:$	**Calculates** $f(N_i^{n+2})$
If received bits =	calculated bits,
$V_n:$	**Calculates** $RTT_n = t_s n - t_r n + T_p$
	$DB_n = \frac{c(RTT_n - T_p)}{2}$
$V_{n+1}:$	**Calculates** $RTT_{n+1} = t_s n + 1 - t_r n + 1 + T_p$
	$DB_{n+1} = \frac{c(RTT_{n+1} - T_p)}{2}$
$V_{n+2}:$	**Calculates** $RTT_{n+2} = t_s n + 2 - t_r n + 2 + T_p$
	$DB_{n+2} = \frac{c(RTT_{n+2} - T_p)}{2}$

3.3.4 Vulnerability Analysis of Trilateration

An attacker knows that it can spoof a distance larger than its actual distance. Therefore, it will look for positions on the highway where it can beguile a verifier into thinking that it is farther away than it actually is. There are two main scenarios each of which can be further sub-divided to four scenarios depending on the positions an attacker can occupy. Figures 3.7 and 3.8 depict the scenarios when attackers are at different parts of a verification unit.

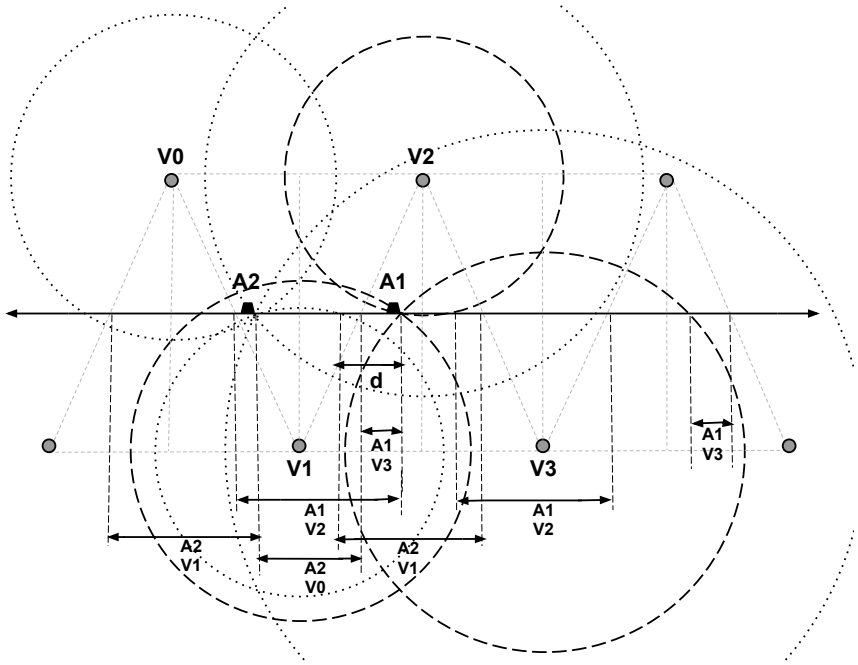


Fig. 3.7: Trilateration, attack scenario I: The attackers (A_1 and A_2) are in adjacent verification units (V_0,V_1,V_2) and (V_1,V_2,V_3).

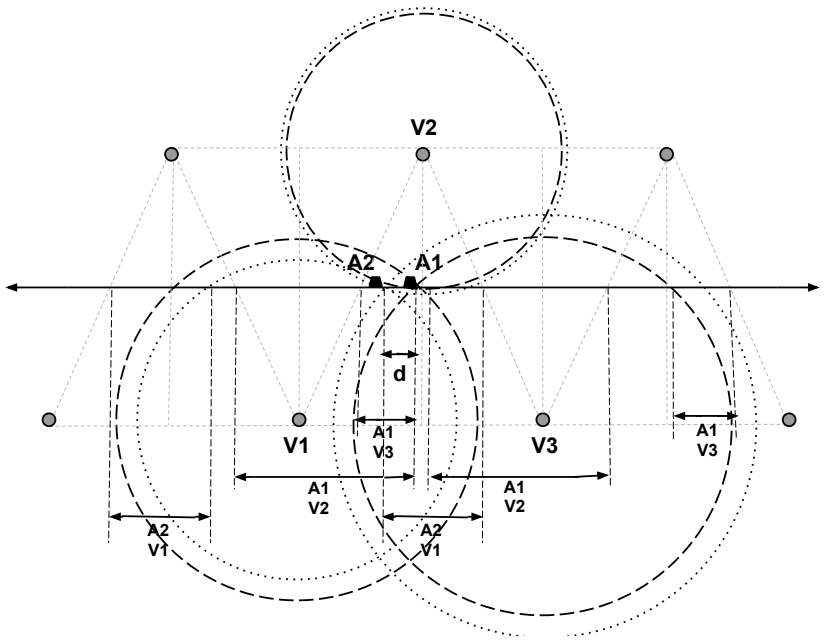


Fig. 3.8: Trilateration, attack scenario II: Both the attackers lie in the same verification unit (V_1,V_2,V_3).

Chapter 4

Friendly Jamming as a Localization Technique

4.1 Introduction to Friendly Jamming

Friendly jamming is a concept of enchancing the security of the physical layer in wireless communications. An eavesdropper can access information from a source sending information to a receiver using the wireless channel. The aim of friendly jamming is to create strategies such that this information is limited only to the receiver while any eavesdropper only receives interference and hence is not able to get the actual useful data. It is assumed that the channels are additive white Gaussian noise (AWGN) channels [49].

There are basically two solutions to increase the secrecy of an information sent by a node to a legitimate receiver.

I: By improving the SNR of the legitimate receiver (e.g. by shortening the distance to the source).

II: By reducing the SNR of the eavesdropper (e.g. by adding controlled interference).

Friendly jamming is based on the second approach. There are three jamming strategies, proposed by Vilela *et al.* [50]. These are:

Blunt jamming: The jammer emits white Gaussian noise with variance at all times. We call this jammer a blunt jammer because it disregards any possible channel state information (CSI) and transmits at a constant power.

Cautious jamming: A cautious jammer takes advantage of the knowledge of the channel state information (CSI) between itself and both the legitimate receiver and the eavesdropper and opportunistically decides when to jam. It jams whenever it has a higher gain to the eavesdropper than to the legitimate receiver, and switches off otherwise.

Adaptive jamming: An adaptive jammer has CSI about the channel to the legitimate receiver only. This strategy corresponds to a situation in which the eavesdropper intercepts

the communications without providing any sign of its presence. In this case, the jammer denes a threshold for the channel quality, above which it will stop jamming since it is likely that his induced noise will hurt the legitimate receiver more than a potential eavesdropper.

Friendly jamming can be implemented for localization in a highway infrastructure by having the transmitter (verifier), legitimate receiver (vehicle under verification), and any eavesdropper (potential attacker) to transmit signals through an additive white Gaussian noise (AWGN) channel, such that the position information sent by a vehicle to the verifier cannot be intercepted by nearby vehicles [51]. Jamming can be achieved by either increasing the signal-to-noise ratio (SNR) of the verifier/legitimate vehicle or by reducing the SNR for nearby vehicles, by introducing controlled interference. Out of the various strategies, blunt jamming is suitable in case of secure localization as in the proposed protocol, we need a high jamming efficiency and lowest possible coverage area [50]. This ensures a secure exchange of information that takes place between a vehicle and a verifier for authenticating the information provided by the vehicle [51].

4.2 Infrastructure Implementing Friendly Jamming

In our proposed secure localization approach, a vehicle proves its position claim by responding to messages from verifiers that can only be received within the locale of the verifiers. To ensure that communication between provers and verifiers can only take place within a certain radius of the verifiers we utilize friendly jamming at the verifiers. To accomplish this, each verifier would employ one set of antennas to transmit the verification message, with a second set placed outside the first and transmitting noise in an outward direction so as to obscure the verification message as shown in Figure 4.1. The granularity of position measurements would depend on the number and spacing of these verifiers. In addition, establishing the veracity of a vehicle's position claim using friendly jamming requires separate channels for communication between the vehicle and a coordinating agent (part of the local verification infrastructure) and the vehicle and two verifiers.

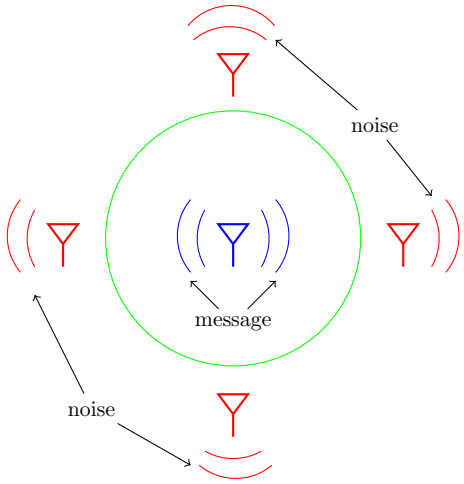


Fig. 4.1: A friendly jamming verifier design using jammers (red) that ensures a verification message (blue) can only be received at the given locality (green circle). A vehicle must lie within this locality to receive a message.

4.3 The Friendly Jamming Protocol

The Protocol 4.1 implements friendly jamming for verification of a location along an infinite highway. First, the vehicle under consideration is queried for its current location, x_0, and velocity, v_0. Having received this information, the infrastructure calculates the time t_1, based on the reported position/velocity and current time, t_0, at which the vehicle should reach the nearest upcoming verifier, V_1 (located at x_1). A random nonce, N_1, is then generated and sent to V_1 along with the time, t_1, at which it should be transmitted. This process is repeated for a second verifier, V_2 (located at x_2), using a new nonce, N_2, and transmit time, t_2. At time t_1 and t_2 the vehicle passes within the range of V_1 and V_2, respectively, and collects N_1 and N_2. To prove its original position claim the vehicle transmits the nonces back to the infrastructure. It is assumed that all communication between the infrastructure and verifiers is encrypted, and that the prover shares secret keys with the infrastructure, K_{IP}, verifier one, K_{V_1P}, and verifier two, K_{V_2P}, for the purposes of authenticating messages.

Protocol 4.1 Verifying a vehicle's location using friendly jamming.

$P \rightarrow I:$	$x_0, v_0, MAC_{K_{IP}}(x_0, v_0)$
$I:$	**Calculate** time $t_1 = \frac{x_1 - x_0}{v_0} + t_0$ at which P reaches V_1 and
$:$	$t_2 = \frac{x_2 - x_0}{v_0} + t_0$ at which P reaches V_2
$I:$	**Generate** random nonces N_1, N_2
$I \rightarrow V_1:$	N_1, t_1
$I \rightarrow V_2:$	N_2, t_2
$V_1:$	**Wait** until t_1
$V_1 \rightarrow P:$	N_{V_1},$MAC_{K_{V_1P}}(N_{V_1})$
$V_2:$	**Wait** until t_2
$V_2 \rightarrow P:$	N_{V_2},$MAC_{K_{V_2P}}(N_{V_2})$
$P \rightarrow I:$	N_{V_1}, N_{V_2},$MAC_{K_{IP}}(N_{V_1}, N_{V_2})$
$I:$	**Verify** x_0, v_0 for P if received nonces match transmitted

4.4 Threat Models for Friendly Jamming

We analyse the friendly jamming infrastructure for two scenarios. Hence, we have two different threat models corresponding to each scenario.

Scenario I: There is one attacker in the system in possession of the identity of one or more legitimate vehicles in the system. In addition, the attacker also has the PV (position and velocity) information of a legitimate vehicle. The goal of the attacker is to use the identity and PV information to pass itself off to a verifier as another legitimate vehicle and hence, falsely localize that legitimate vehicle (spoof) on the highway. The attacker and target vehicle are assumed to travel along the same lane on the highway. For a given vehicle position, the attacker can lie anywhere on the verification segment of the highway to which that position belongs. The attacker is capable of accelerating (or decelerating) upto a given limit. However, it does not have control over its initial position on the highway.

Scenario II: There are two colluding attackers in the system and each attacker targets one verifier in the verification unit. The attackers are in possession of the identity and PV information of one or more legitimate vehicles and they are capable of sharing and using this information. The goal of the attackers is to use the identity and PV information to pass themselves off to each of the two verifiers as one legitimate vehicle and hence, falsely localize that legitimate vehicle (spoof) on the highway. Both of the attackers and target vehicle are assumed to travel along the same lane on the highway. The attackers cannot overtake

any vehicle on the highway. This results in the restriction that the attacker targeting the second verifier must always be ahead of the attacker targeting the first verifier. For a given vehicle position, the attackers can lie anywhere on the verification segment of the highway to which that position belongs. The attackers are capable of accelerating (or decelerating) independently upto a given limit and do not have control over their initial positions on the highway.

4.5 Vulnerability Analysis of Friendly Jamming

For a preliminary analysis of the security of this approach, let us assume that an attacker located at x_a and traveling with a uniform velocity, v_a attempts to spoof the position P by reporting, at time $t = 0$, its location and velocity as x_0 and v_0, respectively (Figure 4.2). Allowing the verifiers,V_1 and V_2 to be located at x_1 and x_2, respectively, at times $t_1 = (x_1 - x_0)/v_0$ and $t_2 = (x_2 - x_0)/v_0$, the verifiers will transmit their respective nonces. The attacker's actual position and velocity must be such that at times t_1 and t_2 they are at x_1 and x_2; x_a , v_a must satisfy $x_1 = x_a + v_a t_1$ and $x_2 = x_a + v_a t_2$. By rearranging these expressions and taking the ratios of t_1 and t_2, we have

$$\frac{t_1}{t_2} = \frac{x_1 - x_0}{x_2 - x_0} = \frac{x_1 - x_a}{x_2 - x_a}, \tag{4.1}$$

which shows that the attacker must be at the position P ($x_a = x_0$) in order to acquire both nonces. Thus, it is not possible for an the attacker traveling at a constant velocity to prove any position but their actual position. In section 5.4, we analyze the case of an attacker with the capability to accelerate or decelerate in order to reach a verifier at the correct time and then we analyze the case when there are two colluding attackers, each capable of accelerating or decelerating independently.

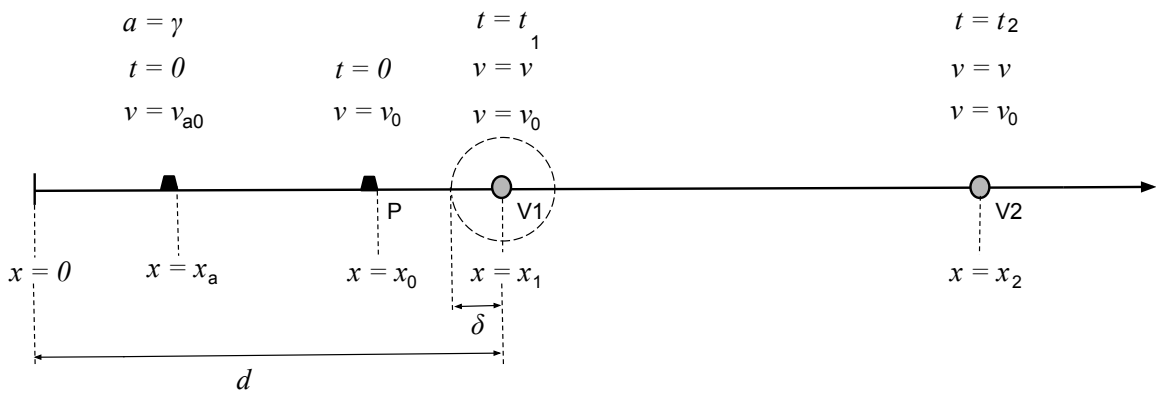


Fig. 4.2: Friendly jamming infrastructure: verifier range = d; verifier scope = d, at time $t = 0$ and $t = t_3$ and δ at time $t = t_1$ and $t = t_2$. In case of a vehicle at position, P: verification unit = V_1, V_2; verification segment = 0 to V_2.

Chapter 5

Spoofing Probability

We have analysed the vulnerability of the architectures using distance bounding, trilateration, and friendly jamming in the previous chapter. Now, we will assign a measure to the vulnerability of each of these infrastructures. For this purpose we define a term known as spoofing probability as follows.

Definition 9 *Spoofing probability*: The likelihood of a verifier calculating the vehicle position of a legitimate vehicle erroneously, due to false information provided by malicious vehicles randomly situated on the highway.

Consider a basic implementation of distance bounding as shown in Figure 3.1. To find the probability of spoofing of a given point on the highway from a given verifier, we can draw analogy from the simple experiment of tossing a coin. For one instance of tossing a coin we have two possible outcomes. Similarly, for a given instance of verifying a position by one verifier there can be a set of two mutually exclusive outcomes, denoted by $X = \{S, S^c\}$, where S indicates that the position of the vehicle can be spoofed while S^c indicates that the position of the vehicle cannot be spoofed.

If the distance of a vehicle from two verifiers, V_m and V_n, are x_m and x_n, respectively, we will have two different sets of outcomes for each verifier. On the assumption that the likelihood of spoofing a point from two different verifiers are independent of each other, the probability of spoofing the vehicle position on a infrastructure using two verifiers is

$$P\left(x = x_m | x = x_n\right) P\left(x = x_n | x = x_m\right) = P\left(x = x_m\right) P\left(x = x_n\right), \tag{5.1}$$

where x is the random variable denoting the distance between a verifier and a point. We use this property to find the probability density function of spoofing for more complex

infrastructures involving multiple verifiers.

The tossing of a coin for a set of trials follows a binomial distribution. However, we cannot use binomial distribution to model the spoofing of a point because in the case of tossing a coin, the probability of a success is always a constant (0.5). However, in case of the spoofing of a point from a set of verifiers, the probability of a success for each verifier depends on the distance of the point from the corresponding verifier. Thus, we can use a Poisson binomial distribution to find the probability of spoofing a point from x verifiers out of a set of n verifiers. This is the case of spoofing a single point in space from a given number of verifiers.

5.1 Sample Space and Probability Density Function

We use σ-algebra to define our sample space and then we assign a probability measure to each element of this sample space. Following the three criteria for a set to be defined as a σ-algebra [52], we consider a set of points, (Σ) lying within the verification scope of a given verifier to be a σ-algebra defined over the set, (Ω) which is the set of all points on the highway. In set-notation,

$$\Omega = x\,(P) \in [0, \infty) \text{ and } \Sigma \subset \Omega \text{ defined by}$$

$$\Sigma = \{y\,(P) \in [0, d] : y\,(P) = |x\,(P) - x\,(V)|\}$$

where

$x\,(P) =$ position of the point, P from $x = 0$,

$x\,(P) =$ position of the verifier, V from $x = 0$, and

$d =$ distance between adjacent verifiers.

The cardinality of the set, Σ, i.e. $\|\Sigma\| = d$, is essentially the verifier scope for the given infrastructure. Suppose the position of the attacker A is at $x(A)$. It can then spoof the point at $x(P)$ from the verifier at $x(V)$ if

$$|x\,(P) - x\,(V)| \leq |x\,(A) - x\,(V)|\,, \tag{5.2}$$

where the value of $|x(P) - x(V)|$ is the spoofing range of P from the verifier V.

Let us consider a platoon of vehicles traveling along the highway-infrastructure assumed for distance bounding. The effective vehicle length of all vehicles are assumed to be the same and equal to L. The spoofing probability is the number of vehicles within the spoofing range divided by the number of vehicles in the sample space, i.e. the verifier scope. Since the leading edge of a vehicle to marks the vehicle position, the number of possible attackers within the scope of a verifier behind the vehicle is $\left\lceil \frac{2x}{L} \right\rceil - 1$. For a verifier in front, the number of possible attackers is $\left\lfloor \frac{2(d-x)}{L} \right\rfloor$.

An attacker can spoof a vehicle's location either from behind or from the front depending on which verifier it is closer to compared to the target vehicle. When a vehicle has crossed a verifier and is still within the verifier scope, an attacker can spoof from behind and the corresponding probability density function is given by

$$P_b(x = P) = \frac{\left\lceil \frac{2x}{L} \right\rceil - 1}{\left\lceil \frac{d+x}{L} \right\rceil + \left\lfloor \frac{d-x}{L} \right\rfloor - 1}. \tag{5.3}$$

Similarly, when a vehicle is approaching a verifier and is currently within the verifier scope, it can be spoofed by an attacker at the front and the corresponding probability density function is given by

$$P_f(x = P) = \frac{\left\lfloor \frac{2(d-x)}{L} \right\rfloor}{\left\lceil \frac{x}{L} \right\rceil + \left\lfloor \frac{2d-x}{L} \right\rfloor - 1}. \tag{5.4}$$

We can verify that these are valid pdfs which follows the axioms of probability [53]. If we consider the effective vehicle length to be infinitesimally small compared to the distances along the highway, the pdf can be calculated by applying a limit to L. For a vehicle spoofing a position to its rear

$$\begin{aligned} \lim_{L \to 0} P_b(x = P) &= \frac{\left\lceil \frac{2x}{L} \right\rceil - 1}{\left\lceil \frac{d+x}{L} \right\rceil + \left\lfloor \frac{d-x}{L} \right\rfloor - 1} = \frac{L \times \left(\left\lceil \frac{2x}{L} \right\rceil - 1 \right)}{L \times \left(\left\lceil \frac{d+x}{L} \right\rceil + \left\lfloor \frac{d-x}{L} \right\rfloor - 1 \right)} \\ &= \frac{2x - L}{(d+x) + (d-x) - L}^{1} = \frac{x}{d}. \end{aligned} \tag{5.5}$$

Similarly, for a vehicle spoofing a forward position

$$\lim_{L \to 0} P_f\left(x = P\right) = \frac{d-x}{d}. \tag{5.6}$$

5.2 Spoofing Probability of the Distance Bounding Infrastructure

There needs to be a minimum of two attackers working simultaneously to spoof the vehicle position from the respective verifiers responsible for localization. As the vehicle moves from the beginning of the verification segment to the end of it, the spoofing probability, P_{DB} is the probability of a position getting spoofed from behind, when it has been spoofed from the front and vice versa. Equation (5.1) can be applied to this case. Therefore,

$$P_{DB} = \frac{x}{d} \times \frac{d-x}{d} = \frac{x\left(d-x\right)}{d^2}. \tag{5.7}$$

We find that the spoofing probability is similar to the beta distribution when the parameters $\alpha = 2, \beta = 2$. The steps used to proof this are as follows. From equation (5.7),

$$P_{DB} = \frac{x}{d} \times \frac{d-x}{d} = \frac{x}{d} \times \left(1 - \frac{x}{d}\right). \tag{5.8}$$

Let $\frac{x}{d} = v$, where $0 \leq v \leq 1$,

$$P_{DB} = v \times \left(1 - v\right). \tag{5.9}$$

The probability distribution function for a beta distribution is given by

$$f\left(v\right) = \frac{1}{B\left(\alpha, \beta\right)} v^{\alpha-1} \times \left(1-v\right)^{\beta-1}. \tag{5.10}$$

Let $\alpha = 2$, $\beta = 2$. Also, the normalizing constant, $\frac{1}{B(\alpha,\beta)}$ is given by

$$B\left(2, 2\right) = \int_0^1 v\left(1-v\right) dv. \tag{5.11}$$

Since, $v = \frac{x}{d} \Rightarrow dv = \frac{1}{d}dx$. And $v \to 1 \Rightarrow x \to d$

$$\begin{aligned} B(2,2) &= \int_0^d \frac{x}{d} \times \left(1 - \frac{x}{d}\right) \frac{1}{d} dx \\ &= \frac{1}{d} \int_0^d \frac{x}{d} - \frac{x^2}{d^2} dx \\ &= \frac{1}{d^3} \left[\frac{3x^2 d - 2x^3}{6}\right]_d^0 \\ &= \frac{1}{6} \\ \Rightarrow f(v) &= 6 \times v \times (1 - v). \end{aligned} \tag{5.12}$$

Comparing equations (5.9) and (5.10),

$$P_{DB} = 6 \times f(v). \tag{5.13}$$

Thus, we can express spoofing probability as a probability distribution function following the beta distribution with $\alpha = 2$, $\beta = 2$, $B(\alpha, \beta) = \frac{1}{6}$ and $v = \frac{x}{d}$ such that $0 \leq v \leq 1$. The mean or expected value is given by

$$mean = \frac{\alpha}{\alpha + \beta}. \tag{5.14}$$

In our case it is calculated to be $v = \frac{1}{2}$ or $x = \frac{d}{2}$. The variance and standard deviation (SD) from the mean is given by

$$\begin{aligned} variance &= \frac{\alpha B}{(\alpha + \beta)^2 (\alpha + \beta + 1)}, \\ SD &= \sqrt{variance}. \end{aligned} \tag{5.15}$$

In our case it is calculated to be $\frac{d\sqrt{variance}}{10}$. Now, we can apply and find out the mean and standard deviation for other infrastructures which use the distance bounding protocol. We use the same steps for the trilateration infrastructure. Figure 5.1 shows the spoofing probability for three distance bounding infrastructures with different values of d (distance between adjacent verifiers).

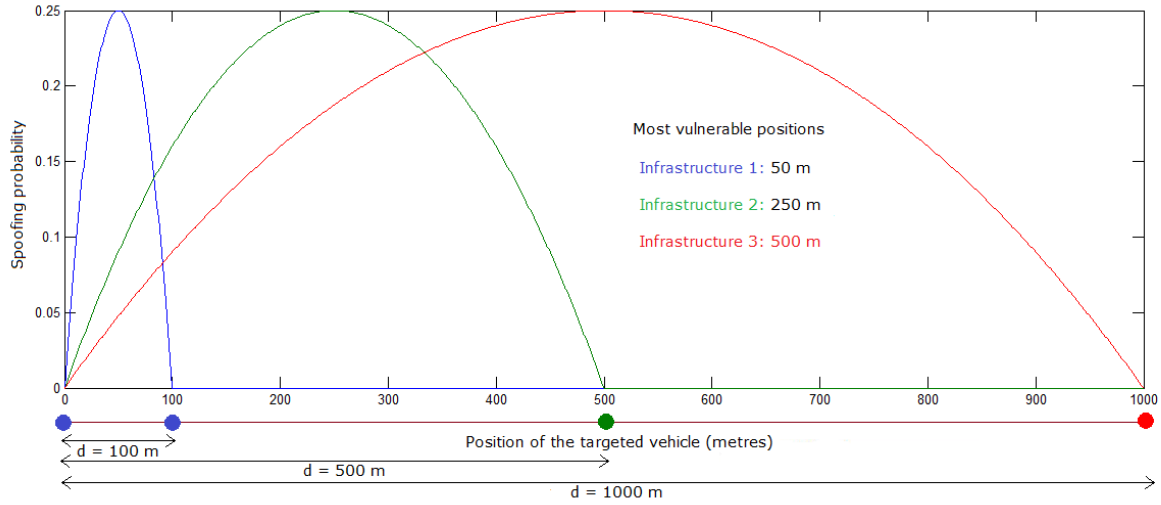


Fig. 5.1: Spoofing probability for three distance bounding infrastructures, schematically drawn below the graph with verifiers in blue, green, and red, as a function of the position of the targeted vehicle as it travels along a verification unit.

5.3 Spoofing Probability of the Verifiable Trilateration Infrastructure

As a vehicle moves along the verification segment in this infrastructure from one end towards the center, the probability of spoofing a position from the front goes on decreasing and becomes zero when the vehicle is right in front of the verifier at the center. If we assume two colluding attackers, one in front and the other at the back, the roles of the attackers switch after the vehicle crosses the center. The spoofing probability for the given trilateration infrastructure is given according to the location of the vehicle within a verification segment.

$$P_b = \frac{\left\lceil \frac{2x}{L} \right\rceil - 1}{\left\lceil \frac{3/2d+x}{L} \right\rceil + \left\lfloor \frac{3/2d-x}{L} \right\rfloor - 1} \text{ for } 0 \leq x \leq d. \tag{5.16}$$

$$P_b = \frac{\left\lceil \frac{2(x-d)}{L} \right\rceil - 1}{\left\lceil \frac{d/2+x}{L} \right\rceil + \left\lfloor \frac{5/2d-x}{L} \right\rfloor - 1} \text{ for } d \leq x \leq 2d. \tag{5.17}$$

$$P_f = \frac{\left\lfloor \frac{2(d-x)}{L} \right\rfloor - 1}{\left\lceil \frac{d/2+x}{L} \right\rceil + \left\lfloor \frac{5/2d-x}{L} \right\rfloor - 1} \text{ for } 0 \leq x \leq d. \tag{5.18}$$

$$P_f = \frac{\left\lfloor \frac{2(2d-x)}{L} \right\rfloor - 1}{\left\lceil \frac{d/2+x}{L} \right\rceil + \left\lfloor \frac{5/2d-x}{L} \right\rfloor - 1} \text{ for } d \leq x \leq 2d. \tag{5.19}$$

As in the case of distance bounding, the probability of spoofing from the front and the back are independent of each other (as they involve two different verifiers). The spoofing probability of a vehicle position is given by the product of probability of spoofing from the front and the back.

$$P_{Trilateration} = P_b \times P_f. \tag{5.20}$$

Figure 5.2 shows the spoofing probability for three distance bounding infrastructures with different values of d (distance between adjacent verifiers).

5.4 Spoofing Probability of the Friendly Jamming Infrastructure

In this method, we consider the sample space as given by equation (5.2). However, the condition for spoofing is different from that of distance bounding and trilateration. An attacker can spoof only those positions which are not already occupied by another vehicle. This is because if a position is occupied by a legitimate vehicle, then this vehicle crosses the verifiers at the times calculated by the verifiers from its position/velocity (PV) information. However, an attacker can spoof a segment along the highway before it reaches the first verifier. In addition to position, the attacker must be able to spoof its velocity so that the times calculated by the false PV information transmitted by the attacker matches with its actual times of crossing. Therefore, the spoofing probability will depend on the attacker's position relative to the target position and also the attacker velocity relative to the target velocity. We will find the spoofing probability as a ratio of the available lengths within the range of velocity differences available for spoofing and the sum of all such lengths as the position changes along the verification unit. According to the threat model described for the friendly jamming infrastructure, we will analyze spoofing in two cases.

Case I: A single attacker verifying for both verifiers.

Case II: Two colluding attackers acting independently to verify for one verifier each. In order to find the available lengths and the range of velocity differences, we should be able

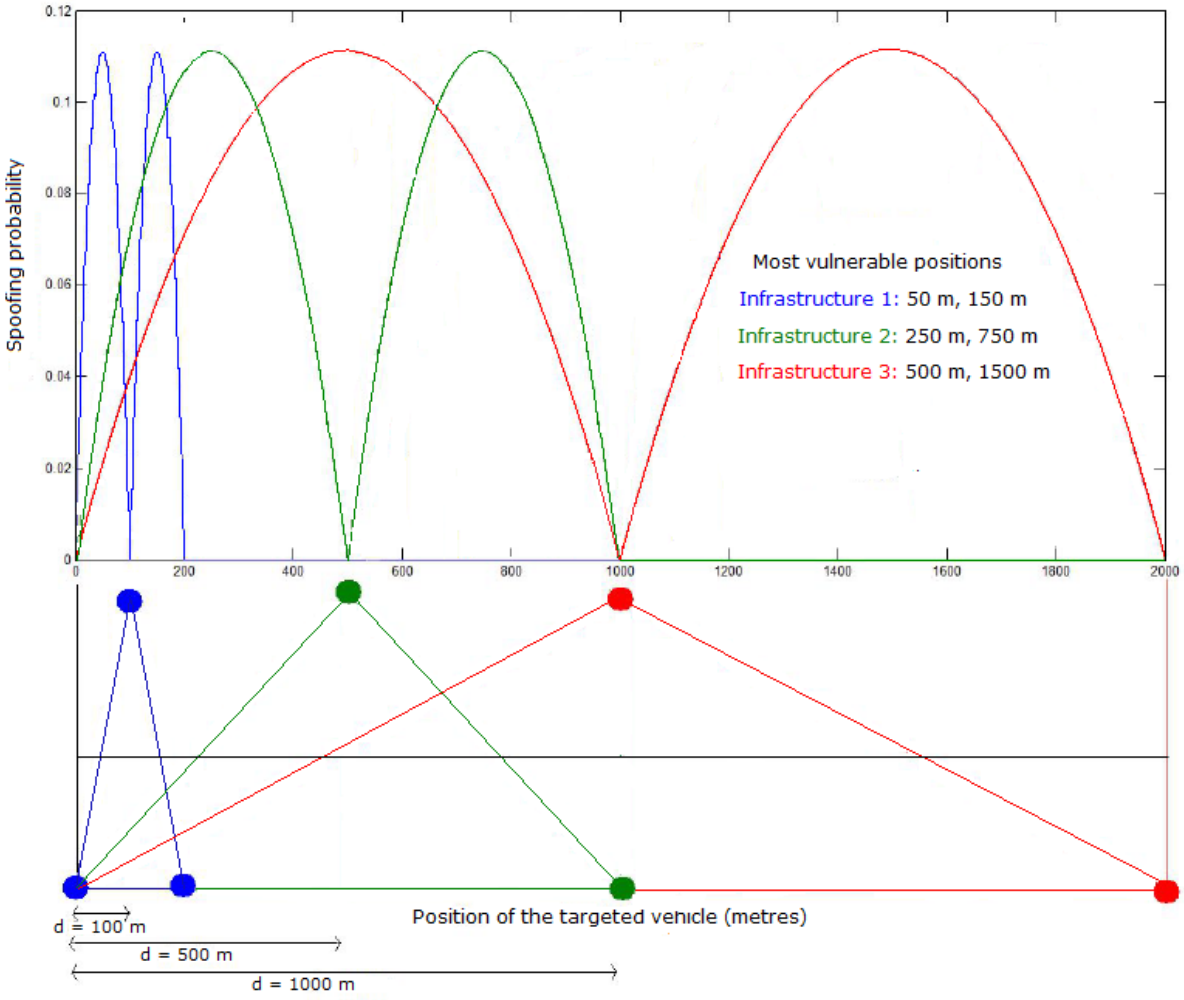


Fig. 5.2: Spoofing probability for three trilateration infrastructures, schematically drawn below the graph with verifiers in blue, green, and red, as a function of the position of the targeted vehicle as it travels along a verification unit.

to establish an upper and lower bound on the difference between the actual and target PV information and then find a condition such that for an instant of verifying a point from a given verifier, the outcome S (that the position cannot be spoofed) is true.

Case I: Single attacker

Let $\{x_0, v_0\}$ be the PV information that an attacker wants to spoof. The infrastructure

determines the times of crossing t_1 and t_2 as

$$\begin{aligned} t_1 &= \frac{x_1 - x_0}{v_0}, \\ t_2 &= \frac{x_2 - x_0}{v_0}. \end{aligned} \tag{5.21}$$

However, the attacker has an actual PV as it travels along the highway. Let its actual PV be denoted by $\{x_a, v_a\}$. The attacker must accelerate or decelerate in order to be able to reach the verifiers on time. Allow a_1 and a_2 to be the accelerations required to reach verifier V_1 in time t_1 and V_2 in time t_2. Equations (5.22) and (5.25) give the motion of the attacker from the beginning of the verification segment (considered to be the origin) to V_1 and then from V_1 to V_2.

$$\begin{aligned} x_1 - x_a &= v_{a0} t_1 + \frac{1}{2} a_1 t_1^2 \\ &= v_{a0} \left(\frac{x_1 - x_0}{v_0} \right) + \frac{1}{2} a_1 \left(\frac{x_1 - x_0}{v_0} \right)^2. \end{aligned} \tag{5.22}$$

As $x_1 = d$, where $d =$ distance between adjacent verifiers,

$$\begin{aligned} d - x_a &= v_a \left(\frac{d - x_0}{v_0} \right) + \frac{1}{2} a_1 \left(\frac{d - x_0}{v_0} \right)^2 \\ \Rightarrow a_1 &= \frac{2 \left[(d - x_a) - v_a \left(\frac{d - x_0}{v_0} \right) \right]}{\left(\frac{d - x_0}{v_0} \right)^2}. \end{aligned} \tag{5.23}$$

Let $x_a - x_0 = \Delta x$ and $v_a - v_0 = \Delta v$

$$\Rightarrow a_1 = -2 \left[\Delta x \left(\frac{v_0}{d - x_0} \right)^2 + \Delta v \left(\frac{v_0}{d - x_0} \right) \right]. \tag{5.24}$$

Using the fact that the vehicle motion from verifier one to two is

$$x_2 - x_1 = v_{a1} (t_2 - t_1) + \frac{1}{2} a_2 (t_2 - t_1)^2, \tag{5.25}$$

and $v_{a1} = v_a + a_1 t_1$, we have

$$\begin{aligned}
\Rightarrow & x_2 - x_1 = (v_a + a_1 t_1)(t_2 - t_1) + \frac{1}{2} a_2 (t_2 - t_1)^2 \\
& = \left[v_a + \left(a_1 - \frac{1}{2} a_2 \right) t_1 + \frac{1}{2} a_2 t_2 \right] (t_2 - t_1) \\
\Rightarrow & (v_0 - v_a) = \left(a_1 - \frac{1}{2} a_2 \right) \left(\frac{x_1 - x_0}{v_0} \right) + \frac{1}{2} a_2 \left(\frac{x_2 - x_0}{v_0} \right).
\end{aligned} \tag{5.26}$$

As $x_2 = 2x_1 = 2d$, the equation reduces to

$$a_2 = \frac{-2 \left[a_1 (d - x_0) + v_0 \Delta v \right]}{d}. \tag{5.27}$$

Finally, substituting the value of a_1

$$a_2 = 2 \left[2 \Delta x \frac{v_0^2}{d (d - x_0)} + \Delta v \frac{v_0}{d} \right]. \tag{5.28}$$

As vehicles are limited in their ability to accelerate and decelerate, allow the magnitude of maximum acceleration to be denoted by γ. The magnitudes of a_1 and a_1 are bounded by γ. Thus,

$$\begin{aligned}
& |a_1| \leq \gamma \\
\Rightarrow & \left| \Delta x \left(\frac{v_0}{d - x_0} \right)^2 + \Delta v \left(\frac{v_0}{d - x_0} \right) \right| \leq \frac{\gamma}{2} \\
\Rightarrow & |\Delta x v_0 + \Delta v (d - x_0)| \leq \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0} \\
\Rightarrow & \pm \left[\Delta x v_0 + \Delta v (d - x_0) \right] \leq \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0} \\
\Rightarrow & \pm \left[\Delta x v_0 \right] \pm \left[\Delta v (d - x_0) \right] \leq \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0}.
\end{aligned} \tag{5.29}$$

Since, v_0 and $d - x_0$ are always positive quantities during the course of the vehicle traveling from $x = 0$ to $x = x_0$, we have

$$|\Delta x| v_0 + |\Delta v| (d - x_0) \leq \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0}. \tag{5.30}$$

Similarly, the bounds on the attacker's acceleration to reach the second verifier is

$$\begin{aligned} &|a_2| \leq \gamma \\ \Rightarrow &2\left|\Delta x\right| v_0 + \left|\Delta v\right| (d - x_0) \leq \frac{\gamma}{2} \frac{d\,(d - x_0)}{v_0}. \end{aligned} \tag{5.31}$$

Considering (5.30) and (5.31), with the limit $\Delta v \to 0$, we find the maximum value of Δx and then considering these equations with limit $\Delta x \to 0$ we find the maximum value of Δv. The range of values for Δx and Δv are given by (5.32) and (5.33).

$$\begin{aligned} 0 < |\Delta x| < \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0^2} \text{ for verifier, } V_1. \\ 0 < |\Delta x| < \frac{\gamma}{4} \frac{d\,(d - x_0)}{v_0^2} \text{ for verifier, } V_2. \end{aligned} \tag{5.32}$$

$$\begin{aligned} 0 < |\Delta v| < \frac{\gamma}{2} \frac{d - x_0}{v_0} \text{ for verifier, } V_1. \\ 0 < |\Delta v| < \frac{\gamma}{2} \frac{d}{v_0} \text{ for verifier, } V_2. \end{aligned} \tag{5.33}$$

In case of friendly jamming, the spoofing probability depends not only in the position, x_0 but also in the target velocity v_0. Let us define the spoofing probability for a constant difference in velocities i.e. $\Delta v = 0, ...v_n..., \Delta v_{max}$, where v_n is an arbitrary value of Δv and Δv_{max} is the maximum value of Δv given by equation (5.33). The formula of spoofing probability for verifier, V_1 when v_0 and Δv are constants and x_0 varies, is given by

$$P_{V_1, v_0, \Delta v}\left(x = x_0, \Delta v = \Delta v_n\right) = \frac{\frac{\gamma}{2} \frac{(d - x_0)^2}{v_0^2} - \Delta v_n \frac{(d - x_0)}{v_0}}{\sum_{x_0=0}^{d} \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0^2} - \Delta v_n \frac{(d - x_0)}{v_0}}. \tag{5.34}$$

Similarly, we can find the spoofing probability for verifier, V_2, considering the above steps and using the corresponding expressions for Δv and Δx from equation (5.32) and (5.33). The formula is given by

$$P_{V_2, v_0, \Delta v}\left(x = x_0, \Delta v = \Delta v_n\right) = \frac{\frac{\gamma}{4} \frac{d(d - x_0)}{v_0^2} - \Delta v_n \frac{(d - x_0)}{2v_0}}{\sum_{x_0=0}^{d} \frac{d(d - x_0)}{v_0^2} - \Delta v_n \frac{(d - x_0)}{2v_0}}. \tag{5.35}$$

The equation (5.34) can be expanded into the following steps for ease of computation.

$$P_{\Delta v=0}\left(x=x_0, v=v_0\right) = P\left(|\Delta x| < \frac{\gamma}{2}\frac{\left(d-x_0\right)^2}{v_0^2}\right) = P\left(|\Delta x| < \Delta x_{max}\right)$$

$$\vdots$$

$$P_{\Delta v=v_n}\left(x=x_0, v=v_0\right) = P\left(|\Delta x| < \frac{\gamma}{2}\frac{\left(d-x_0\right)^2}{v_0^2} - \Delta v_n\frac{(d-x_0)}{v_0}\right)$$

$$\vdots$$

$$\begin{aligned} P_{\Delta v=v_{max}}\left(x=x_0, v=v_0\right) &= P\left(|\Delta x| < \frac{\gamma}{2}\frac{\left(d-x_0\right)^2}{v_0^2} - \Delta v_{max}\frac{(d-x_0)}{v_0}\right) \\ &= P\left(|\Delta x| < \Delta x_{max} - \Delta v_{max}\frac{(d-x_0)}{v_0}\right) \\ &= P\left(|\Delta x| < 0\right). \end{aligned}$$

The spoofing probability for verifier, V_1, when Δv varies along with x is given by

$$P\left(x=x_0, v=v_0\right) = P\left(|\Delta x| < \frac{\gamma}{2}\frac{\left(d-x_0\right)^2}{v_0^2} - \Delta v\frac{(d-x_0)}{v_0}\right). \tag{5.36}$$

If v_0 is kept constant, the bounds for Δx in the RHS depends on two variables, i.e. x_0 and Δv. Now, the formula for spoofing probability is given by

$$P_{V_1,v_0} = \frac{\frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} - \Delta v_n\frac{(d-x_0)}{v_0}}{\sum_{\Delta v=0}^{\Delta v_{max}}\sum_{x_0=0}^{d}\frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} - \Delta v_n\frac{(d-x_0)}{v_0}}. \tag{5.37}$$

The spoofing probability for both V_1 and V_2 is given by

$$P_{V_1,v_0,\Delta v}\bigcap P_{V_2,v_0,\Delta v} = P(V_2|V_1)P(V_1). \tag{5.38}$$

From equation (5.25) and (5.26), we know that the bounds for V_2 is calculated assuming that the attacker has already crossed V_1. Hence, $P(V_2|V_1) = P_{V_2,v_0,\Delta v}$, $P(V_1) = P_{V_1,v_0,\Delta v}$ and

$$P_{V_1,v_0,\Delta v} \bigcap P_{V2,v_0,\Delta v} = P_{V_1,v_0,\Delta v}.P_{V_2,v_0,\Delta v}. \tag{5.39}$$

Case II: Two colluding attackers

Let $\{x_0, v_0\}$ be the PV information that two colluding attackers, A_1 and A_2, want to spoof. Let us assume that A_1 targets the first verifier, V_1, and A_2 targets the second verifier, V_2. The motion of these attackers are independent, i.e. their acceleration can be different and depends only on their position and velocity with respect to the target PV information. Let a_{A_1} be the acceleration of A from $x = 0$ to $x = d$ (position of V_1) and a_{A_2} be the acceleration of A_2 from $x = 0$ to $x = 2d$ (position of V_2). The equation of motion for A_1 would be same as that of a single attacker trying to reach V_1 at time t_1. It is given by equation (5.22). Therefore, for the attacker, A_1, we have

$$\begin{aligned} x_1 - x_{A_1} &= v_{A_1 0} t_1 + \frac{1}{2} a_{A_1} t_1^2 \\ &= v_{A_1 0} \left(\frac{x_1 - x_0}{v_0} \right) + \frac{1}{2} a_{A_1} \left(\frac{x_1 - x_0}{v_0} \right)^2, \end{aligned} \tag{5.40}$$

which finally results in

$$\Rightarrow a_A = -2 \left[\Delta x \left(\frac{v_0}{d - x_0} \right)^2 + \Delta v \left(\frac{v_0}{d - x_0} \right) \right]. \tag{5.41}$$

Now, the attacker, A_2, has to cover a distance $x_2 - x_{A_2} = 2d$ in time t_2, which gives the following equations.

$$\begin{aligned} x_1 - x_{A_2} &= v_{A_2 0} t_2 + \frac{1}{2} a_{A_2} t_2^2 \\ = v_{A_2 0} \left(\frac{x_2 - x_0}{v_0} \right) &+ \frac{1}{2} a_{A_2} \left(\frac{x_2 - x_0}{v_0} \right)^2, \end{aligned} \tag{5.42}$$

which finally results in

$$\Rightarrow a_{A_2} = -2\left[\Delta x\left(\frac{v_0}{2d-x_0}\right)^2 + \Delta v\left(\frac{v_0}{2d-x_0}\right)\right]. \tag{5.43}$$

This finally results in the following bounds in position (Δx_{A_1} and Δx_{A_2}) and bounds in velocity (Δv_{A_1} and Δv_{A_2}) for attackers A_1 and A_2. It is similar to equation (5.30). We have

$$|\Delta x_{A_1}|\, v_0 + |\Delta v_{A_1}|\,(d-x_0) \leq \frac{\gamma}{2}\frac{(d-x_0)^2}{v_0}. \tag{5.44}$$

And for attacker A_2 (by replacing d with 2d) we have

$$|\Delta x_{A_2}|\, v_0 + |\Delta v_{A_2}|\,(2d-x_0) \leq \frac{\gamma}{2}\frac{(2d-x_0)^2}{v_0}. \tag{5.45}$$

The maximum values are given by

$$\begin{aligned} 0 < |\Delta x_{A_1}| &< \frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} \text{ for verifier, } V_1 \\ 0 < |\Delta x_{A_2}| &< \frac{\gamma}{2}\frac{(2d-x_0)^2}{v_0^2} \text{ for verifier, } V_2, \end{aligned} \tag{5.46}$$

$$\begin{aligned} 0 < |\Delta v_{A_1}| &< \frac{\gamma}{2}\frac{d-x_0}{v_0} \text{ for verifier, } V_1 \\ 0 < |\Delta v_{A_2}| &< \frac{\gamma}{2}\frac{2d-x_0}{v_0} \text{ for verifier, } V_2. \end{aligned} \tag{5.47}$$

The formula of spoofing probability for verifier, V_1 by A_1, when v_0 and Δv are constants and x_0 varies, is given by

$$P_{A_1,v_0,\Delta v}\left(x = x_0, \Delta v = \Delta v_n\right) = \frac{\frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} - \Delta v_n\frac{(d-x_0)}{v_0}}{\sum_{x_0=0}^{d}\frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} - \Delta v_n\frac{(d-x_0)}{v_0}}. \tag{5.48}$$

The formula of spoofing probability for verifier, V_2 by A_2, when v_0 and Δv are constants and x_0 varies, is given by

$$P_{A_2,v_0,\Delta v}\left(x = x_0, \Delta v = \Delta v_n\right) = \frac{\frac{\gamma}{2}\frac{(2d-x_0)^2}{v_0^2} - \Delta v_n \frac{(2d-x_0)}{v_0}}{\sum_{x_0=0}^{2d} \frac{\gamma}{2}\frac{(2d-x_0)^2}{v_0^2} - \Delta v_n \frac{(2d-x_0)}{v_0}}. \tag{5.49}$$

Since, A_1 needs to reach V_1 before A_2 needs to reach V_2, there is this restriction that A_2 is always ahead of A_1. This implies that $A_2(x) > A_1(x)$ where $A_1(x)$, $A_2(x)$ are the positions of A_1, A_2 along the highway. The probability that the position is spoofed from both V_1 and V_2 is

$$\begin{aligned}
&P_{A_1,v_0,\Delta v} \bigcap P_{A_2,v_0,\Delta v} \\
&= P_{A_1,v_0,\Delta v}|_{x=0}(P_{A_2,v_0,\Delta v}|_{x=1} + P_{A_2,v_0,\Delta v}|_{x=2} + \ \cdot\ \cdot\ \cdot\ + \\
&P_{A_2,v_0,\Delta v}|_{x=x_n} + \ \cdot\ \cdot\ \cdot\ + P_{A_2,v_0,\Delta v}|_{x=2d}) + \\
&P_{A_1,v_0,\Delta v}|_{x=1}(P_{A_2,v_0,\Delta v}|_{x=2} + P_{A_2,v_0,\Delta v}|_{x=3} + \ \cdot\ \cdot\ \cdot\ + \\
&P_{A_2,v_0,\Delta v}|_{x=x_n} + \ \cdot\ \cdot\ \cdot\ + P_{A_2,v_0,\Delta v}|_{x=2d}) + \\
&P_{A_1,v_0,\Delta v}|_{x=2}(P_{A_2,v_0,\Delta v}|_{x=3} + P_{A_2,v_0,\Delta v}|_{x=4} + \ \cdot\ \cdot\ \cdot\ + \\
&P_{A_2,v_0,\Delta v}|_{x=x_n} + \ \cdot\ \cdot\ \cdot\ + P_{A_2,v_0,\Delta v}|_{x=2d}) + \\
&\qquad\qquad \cdot \\
&\qquad\qquad \cdot \\
&\qquad\qquad \cdot \\
&+P_{A_1,v_0,\Delta v}|_{x=d}(P_{A_2,v_0,\Delta v}|_{x=d+1} + P_{A_2,v_0,\Delta v}|_{x=d+2} + \ \cdot\ \cdot\ \cdot\ + \\
&P_{A_2,v_0,\Delta v}|_{x=d+x_n} + \ \cdot\ \cdot\ \cdot\ + P_{A_2,v_0,\Delta v}|_{x=2d})
\end{aligned}$$

Figures 5.3 and 5.4 represent spoofing probability of a single attacker targeting the verifiers, V_1 and V_2, respectively, and Figure 5.5 represents the spoofing probability of a single attacker targeting both the verifiers, V_1 and V_2. The positions are marked from the origin, $x = 0$. The separation distance (d) between verifiers is 100 metres with the first verifier at $x = 100$. We observe that the spoofing probability of distance bounding and triangulation exhibits the properties similar to the beta distribution when $\alpha = 2$ and $\beta = 2$,

while friendly jamming is similar to the beta distribution when $\alpha = 1$ and $\beta = 3$. Figure 5.6 represents the spoofing probability of a second attacker, A_2, targeting the verifier, V_2. This attacker may collude with A_1, targeting V_1 to spoof a position from the verification system. Figure 5.7 represents spoofing probability of two colluding attackers, A_1 and A_2, targeting the verifiers, V_1 and V_2, respectively. The spoofing probability for a constant Δv is independent of the maximum allowable acceleration. It is only dependant on the range of distances $\Delta x = 0$ to Δx_{max}. This allows us to compare the spoofing probability of friendly jamming with distance bounding and trilateration. If we consider the range of velocities, i.e. $\Delta v = 0$ to Δv_{max}, then the spoofing probability changes with the maximum allowable acceleration, γ. Figure 5.8 represents the spoofing probability of attacker, A_1 spoofing verifier V_1 when both the velocity and position of A_1 varies with respect to the target velocity and position.

5.5 Value of Spoofing Probability

We have analysed the above methods by first defining a threat model and then finding out vulnerabilitiees of each infrastructure. These vulnarabilities decide how easy or difficult it is to attack a given system. We cannot compare two methods as different as distance bounding and friendly jamming or even methods as similar as distance bounding and trilateration unless we assign a measure to the vulnerability of each method to a particular threat model. The idea of probability of an attacker spoofing an arbitaray point, randomly selected along the highway, is the simplest way to find the vulnerability of the infrastructure at that point. Calculating the probability at all such points gives us an overall idea of how effective the localization method is for the defined threat model. Spoofing probability is essentially a measurement to be considered during system development. According to an article by National Institute of Standards and Measurements (NIST), in the various measurements carried out during system development, the measurement of spoofing probability fits in with the measurement carried out in the implementation assessment phase [54]. The value of measurements like spoofing probability, according to the article by NIST, lies in these points.

I: Provides insights into the risk of the system being exploited when implemented.

II: Indicates need for additional security controls in operations.

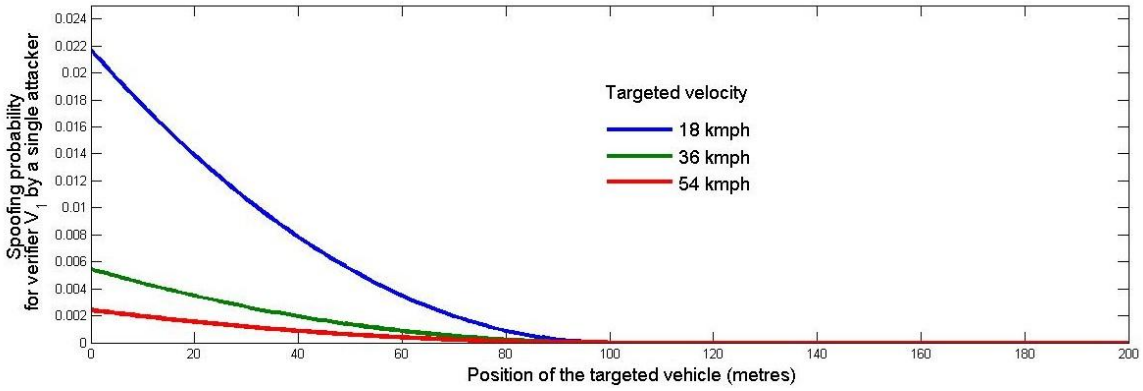


Fig. 5.3: Spoofing probability with $\Delta v = 0$ and constant target velocities (v_0) for the verifier, V_1 by a single attacker, as a function of the position of the targeted vehicle as it travels along a verification unit.

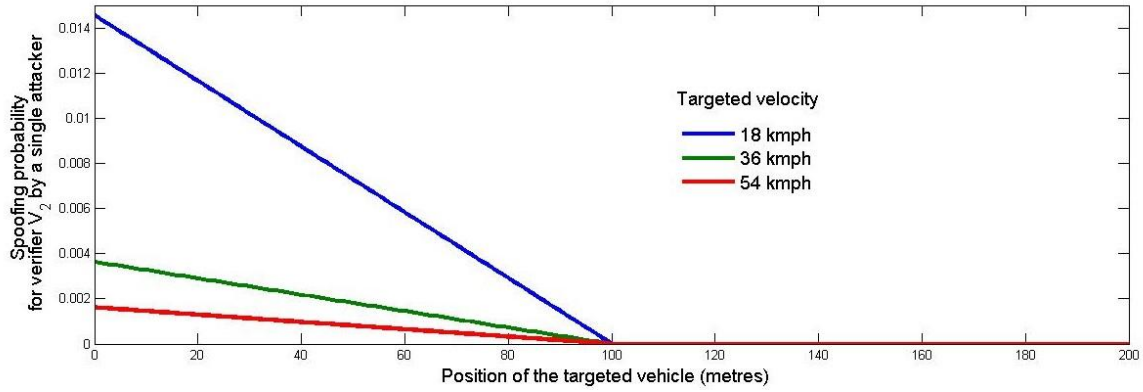


Fig. 5.4: Spoofing probability with $\Delta v = 0$ and constant target velocities (v_0) for the verifier, V_2 by a single attacker, as a function of the position of the targeted vehicle as it travels along a verification unit.

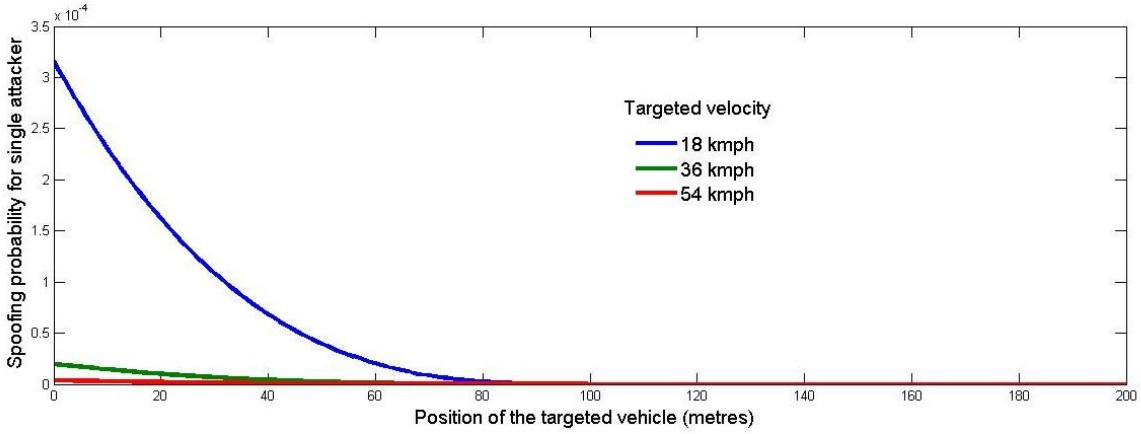


Fig. 5.5: Spoofing probability with $\Delta v = 0$ and constant target velocities (v_0) for a verification unit in the friendly jamming infrastructure by a single attacker, as a function of the position of the targeted vehicle as it travels along a verification unit.

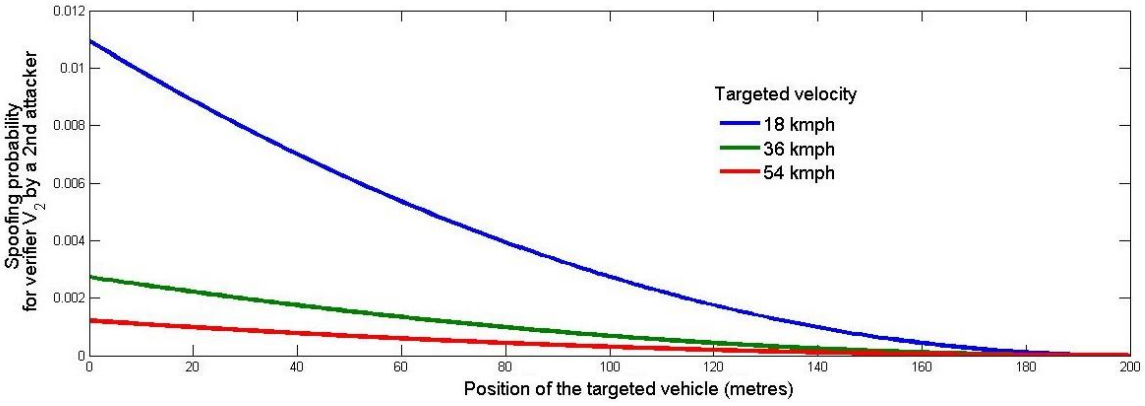


Fig. 5.6: Spoofing probability with $\Delta v = 0$ and constant target velocities (v_0) for the verifier, V_2 by a second attacker, colluding with an attacker targeting the verifier, V_1 as a function of the position of the targeted vehicle as it travels along a verification unit.

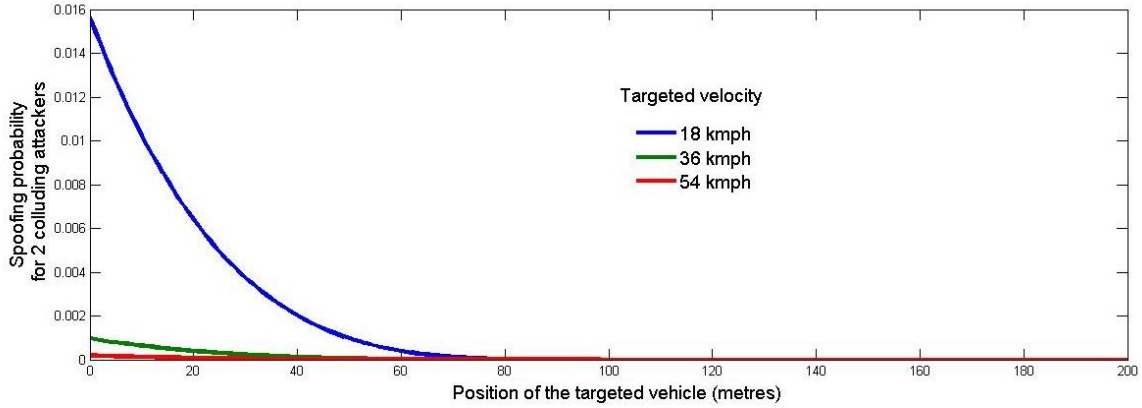


Fig. 5.7: Spoofing probability with $\Delta v = 0$ and constant target velocities (v_0) for a verification unit in the friendly jamming infrastructure by two colluding attackers, as a function of the position of the targeted vehicle as it travels along a verification unit.

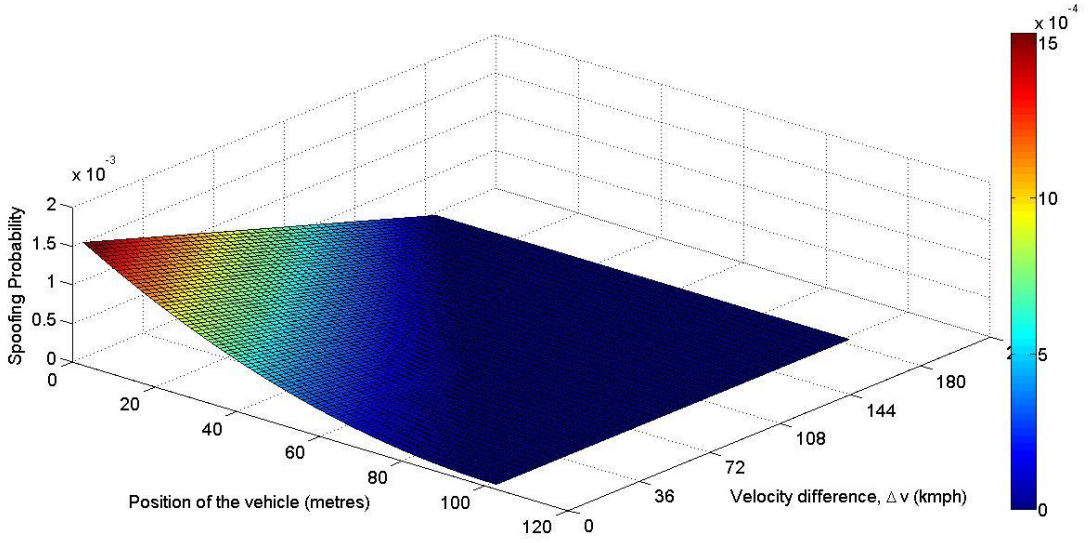


Fig. 5.8: Spoofing probability with $\Delta v = 0$ to Δv_{max} and target velocity, $v_0 = 36$ kmph for the verifier, V_1 by a single attacker, as a function of Δv and the position of the targeted vehicle as it travels along a verification unit.

Chapter 6

Results and Conclusion

We plotted the spoofing probabilities for distance bounding, trilateration and friendly jamming. The results are summarized in Figure 6.1. We observe that, in case of distance bounding, adding more verifiers (trilateration needs three verifiers as opposed to simple distance bounding), the reduces the spoofing probability. However, the expected distance, i.e. mean of all the distances available for spoofing remains the same. Also, the standard deviation (SD), i.e. the average of the square of differences between mean and available distances does not change. Ninety-five percent of the most vulnerable positions lie within the range given by $mean \pm 1.96SD$. Thus, we can determine a range of positions which are more vulnerable compared to other positions along the highway. And this gives us the opportunity to monitor those regions to detect attacks.

Distance between Verifiers, d (m)	Distance Bounding		Trilateration	
	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)
100	0.25	27.64 to 72.36	0.11	27.64 to 72.36
500	0.25	138.2 to 361.8	0.11	27.64 to 72.36
1000	0.25	276.4 to 723.6	0.11	27.64 to 72.36
$d = 100$ m, $\Delta v = 0$, $\Delta x = 0$ to Δx_{max} Spoofing Probability is independent of γ				
Targeted velocity, v_0 (kmph)	Friendly Jamming with 1 attacker		Friendly Jamming with 2 attackers	
	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)
18	3.16×10^{-4}	0 to 5.3709	0.016	0 to 98.389
36	1.97×10^{-5}	0 to 1.3134	9.77×10^{-4}	0 to 21.365
54	3.9×10^{-6}	0 to 0.581	1.93×10^{-4}	0 to 9.029

Fig. 6.1: Comparison of distance bounding, trilateration, and friendly jamming.

Figure 6.2 shows the spoofing probability and vulnerable positions when both the velocity and position of the attacker is considered to differ from the target velocity and position. We consider different allowable acceleration limits, i.e. $\gamma = 1m/s^2$, $5m/s^2$ and $10m/s^2$. Apart from the differences in spoofing probability, there are some basic differences between distance bounding, trilateration, and friendly jamming. Figure 6.3 gives a brief comparison of other aspects of the three localization methods.

6.1 Advantages and Drawbacks of the Friendly Jamming Method

The major advantage of friendly jamming is that the spoofing probability depends not only on the target position, but also the target velocity. In other words, to be able to defeat

d = 100 m, $\Delta v = 0$ to Δv_{max}, $\Delta x = 0$ to Δx_{max}, $\gamma = 1$ m/s^2				
Targeted velocity, v_0 (kmph)	Friendly Jamming with 1 attacker		Friendly Jamming with 2 attackers	
	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)
18	7.52×10^{-4}	0 to 3.989	0.0372	0 to 100
36	7.29×10^{-4}	0 to 4.044	0.0361	0 to 100
54	7.18×10^{-4}	0 to 4.093	0.0356	0 to 100
d = 100 m, $\Delta v = 0$ to Δv_{max}, $\Delta x = 0$ to Δx_{max}, $\gamma = 5$ m/s^2				
Targeted velocity, v_0 (kmph)	Friendly Jamming with 1 attacker		Friendly Jamming with 2 attackers	
	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)
18	7.72×10^{-4}	0 to 3.939	0.0382	0 to 100
36	7.67×10^{-4}	0 to 3.953	0.0379	0 to 100
54	7.62×10^{-4}	0 to 3.965	0.0377	0 to 100
d = 100 m, $\Delta v = 0$ to Δv_{max}, $\Delta x = 0$ to Δx_{max}, $\gamma = 10$ m/s^2				
Targeted velocity, v_0 (kmph)	Friendly Jamming with 1 attacker		Friendly Jamming with 2 attackers	
	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)	Max Spoofing Probability	Most vulnerable position (m) (mean $\pm$ SD)
18	7.74×10^{-4}	0 to 3.931	0.0383	0 to 100
36	7.71×10^{-4}	0 to 3.938	0.0382	0 to 100
54	7.69×10^{-4}	0 to 3.946	0.0381	0 to 100

Fig. 6.2: Friendly jamming with velocity and position of the attacker different from the target velocity and position.

Property	Distance Bounding	Trilateration	Friendly Jamming with 1 attacker	Friendly Jamming with 2 attackers
No. of verifiers in a verification unit	2	3	2	2
Minimum number of attackers required	2	2	1	2
Variables affecting spoofing probability	Distance from each Verifier in a verification unit	Distance from two Verifiers in a verification unit	Distance from each Verifier in a verification unit, Difference between targeted velocity and attacker's velocity	Distance of each attacker from each Verifier in a verification unit, Difference between targeted velocity and each attacker's velocity
Type of Localization	Range-Based	Range-Based and Geometric	Range-Free	Range-Free
Hardware requirements	Transceiver, Encryption device	Transceiver, Encryption device	Short-Range Transceiver, Jammer, Encryption device	Short-Range Transceiver, Jammer, Encryption device

Fig. 6.3: Summary of distance bounding, trilateration, and friendly jamming.

the verification method, the attackers will have to consider the target PV information and not just the position information (P). The attacker will need fast computing hardware in order to get more information about the spoofing probability at that time instant. Also, it is much more difficult to synchromize both position and velocity (that Δx and Δv are within favorable limits for the attacker), than to station oneself in a favorable position in case of distance bounding and trilateration. We observe that due to these restrictions, the spoofing probability for friendly jamming is much less than those of distance bounding. When the distance between adjacent verifiers is 100 meters, friendly jamming achieves a spoofing probability of less than 2%. The equivalent spoofing probabilities for distance bounding is 25% and trilateration is 11%.

A drawback of friendly jamming is because of its large standard deviation of the positions most vulnerable to spoofing. The standard deviation of a probability distribution which decreases slowly on moving away from the mean, would be higher as compared to that

of a probability distribution which decreases rapidly on moving away from the mean. The spoofing probability in case of friendly jamming is more uniform throughout the verification segment, even though is much lesser than that of distance bounding and trilateration. It is to be noted that no localization algorithm can be 100% secure. There are certain attacker configurations for which a position can be certainly spoofed, i.e. the spoofing probability is 1. This is also true with friendly jamming.

6.2 Future Scope

As the currently defined infrastructure using friendly jamming is vulnerable over a large range of distances, there is scope for defining an infrastructure which is more robust in terms of the range of spoofable distances. By modifying the friendly jamming algorithm, we can attempt to improve the spoofing probability and its probability distribution further. We can also compare friendly jamming with other localization methods used in ATS. Currently, we have presented the analysis with a single-lane highway. There is scope for further analysis with multiple-lane highways and how the results differ from the current results. Also, our current analysis gives us the spoofing probability when the attacker's position is unknown, i.e. an attacker can be at any arbitrary position along the highway. If we possess the knowledge of an attacker's position, we can find the spoofing probability for that particular configuration of attackers. For certain configurations, the spoofing probability is 1. We can find such configurations and explore an extension of the friendly jamming method to lower this probability (for example, by adding more verifiers or through continuous monitoring).

References

[1] R. J. Weiland and L. B. Purser, "You have come a long way, ITS," *Transportation research circular on the status and future prospects of intelligent transportation systems*, 2011. http://onlinepubs.trb.org/onlinepubs/millennium/00058.pdf

[2] United States Department of Transportation. http://www.its.dot.gov/its_program/about_its.html

[3] European Union Transportation projects. http://ec.europa.eu/transport/themes/its/

[4] Hong Kong Transportation Department. http://www.td.gov.hk/en/transport_in_hong_kong/its/

[5] Land Transport Authority Singapore. http://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion/intelligent-transport-systems.html

[6] Department of Infrastructure and Transport Australia. http://www.infrastructure.gov.au/transport/its/

[7] E. Coelingh and S. Solyom, "All aboard the robotic road train," *Spectrum, IEEE*, vol. 49, no. 11, pp. 34–39, 2012.

[8] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[9] J. Jiang, G. Han, C. Zhu, Y. Dong, and N. Zhang, "Secure localization in wireless sensor networks: a survey," *IEEE Journal of Communications*, vol. 6, no. 6, pp. 460–470, 2011.

[10] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*. Heidelberg, Berlin, Germany: Springer, 2002, pp. 251–260.

[11] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless sensor networks*. Heidelberg, Berlin, Germany: Springer, ch. 1, pp. 3–12, 2004.

[12] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[13] V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: a survey," in *International Conference on Advanced Information Networking and Applications Workshops, WAINA*, 2009.

[14] M. A. Moharrum and A. A. Al Daraiseh, "Toward secure vehicular ad-hoc networks: a survey," *IETE Technical Review*, vol. 29, no. 1, p. 80, 2012.

[15] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (vanets): challenges and perspectives," in *6th International Conference on ITS Telecommunications, Proceedings*, 2006.

[16] Vehicle Safety Communications Consortium, "Vehicle safety communications project: task 3 final report: identify intelligent vehicle safety applications enabled by dsrc," *National Highway Traffic Safety Administration, US Department of Transportation, Washington DC*, 2005.

[17] Car 2 Car Communication Consortium, "Car 2 car communication consortium manifesto," *Braunschweig, November*, 2007.

[18] J. Fukuyama, "Probabilistic routing for vehicular ad hoc network," Japan Patent 4,807,471, Feb. 21, 2010.

[19] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, and A. Kung, "Secure vehicular communication systems: implementation, performance, and research challenges," *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 110–118, 2008.

[20] A. Boukerche, H. A. Oliveira, E. F. Nakamura, and A. A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," *Computer Communications*, vol. 31, no. 12, pp. 2838–2849, 2008.

[21] A. Benslimane, "Localization in vehicular ad hoc networks," in *Systems Communications, Proceedings*, 2005.

[22] F. Viani, L. Lizzi, P. Rocca, M. Benedetti, M. Donelli, and A. Massa, "Object tracking through rssi measurements in wireless sensor networks," *Electronics Letters*, vol. 44, no. 10, pp. 653–654, 2008.

[23] R. Parker and S. Valaee, "Vehicular node localization using received-signal-strength indicator," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3371–3380, 2007.

[24] R. Parker and S. Valaee, "Vehicle localization in vehicular networks," in *64th Vehicular Technology Conference*, 2006.

[25] S. Venkatraman, J. Caffery Jr., and H.-R. You, "Location using los range estimation in nlos environments," in *55th Vehicular Technology Conference*, 2002.

[26] D. D. McCrady, L. Doyle, H. Forstrom, T. Dempsey, and M. Martorana, "Mobile ranging using low-accuracy clocks," *IEEE Transactions on Microwave Theory and Techniques*, vol. 48, no. 6, pp. 951–958, 2000.

[27] T. Mogi and T. Ohtsuki, "Toa localization using rss weight with path loss exponents estimation in nlos environments," in *14th Asia-Pacific Conference on Communications, APCC*, 2008.

[28] T. Hui, W. Shuang, and X. Huaiyao, "Localization using cooperative aoa approach," in *International Conference on Wireless Communications, Networking and Mobile Computing, WiCom*, 2007.

[29] J. Xu, M. Ma, and C. L. Law, "Aoa cooperative position localization," in *Global Telecommunications Conference, GLOBECOM*, 2008.

[30] Y.-T. Chan, W.-Y. Tsui, H.-C. So, and P.-c. Ching, "Time-of-arrival based localization under nlos conditions," in *IEEE Transactions on Vehicular Technology*, 2006.

[31] S. Venkatraman and J. J. Caffery, "Multipath-aided location estimation using angles of arrival," in *Proceedings of International Society for Optics and Photonics*, 2003.

[32] Y. Shang and W. Ruml, "Improved mds-based localization," in *23rd Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM*, 2004.

[33] Y. Shang, W. Ruml, Y. Zhang, and M. P. Fromherz, "Localization from mere connectivity," in *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, 2003.

[34] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," *Telecommunication Systems*, vol. 22, no. 1-4, pp. 267–280, 2003.

[35] D. Niculescu and B. Nath, "Ad hoc positioning system," in *Global Telecommunications Conference, GLOBECOM*, 2001.

[36] M. G. Dissanayake, P. Newman, S. Clark, H. F. Durrant-Whyte, and M. Csorba, "A solution to the simultaneous localization and map building (slam) problem," *IEEE Transactions on Robotics and Automation*, vol. 17, no. 3, pp. 229–241, 2001.

[37] E. Jose and M. D. Adams, "Millimetre wave radar spectra simulation and interpretation for outdoor slam," in *International Conference on Robotics and Automation, ICRA*, 2004.

[38] G. Anousaki and K. J. Kyriakopoulos, "A dead-reckoning scheme for skid-steered vehicles in outdoor environments," in *International Conference on Robotics and Automation, ICRA*, 2004.

[39] H. Choset and K. Nagatani, "Topological simultaneous localization and mapping (slam): toward exact localization without explicit localization," *IEEE Transactions on Robotics and Automation*, vol. 17, no. 2, pp. 125–137, 2001.

[40] J. E. Guivant and E. M. Nebot, "Optimization of the simultaneous localization and map-building algorithm for real-time implementation," *IEEE Transactions on Robotics and Automation*, vol. 17, no. 3, pp. 242–257, 2001.

[41] F. Bai and B. Krishnamachari, "Exploiting the wisdom of the crowd: localized, distributed information-centric vanets," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 138–146, 2010.

[42] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 427–450, 2009.

[43] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero III, R. L. Moses, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *Signal Processing Magazine*, vol. 22, no. 4, pp. 54–69, 2005.

[44] F. Gustafsson and F. Gunnarsson, "Positioning using time-difference of arrival measurements," in *IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP*, 2003.

[45] S. Qing, *Information and Communications Security: 11th International Conference, ICICS 2009*. Heidelberg, Berlin, Germany: Springer, ch. 3, pp. 92–98, 2010.

[46] F. Stajano, C. Meadows, S. Capkun, and T. Moore, "Secure localization in wireless sensor networks," in *Security and Privacy in Ad-hoc and Sensor Networks: 4th European Workshop, ESAS*, 2007.

[47] S. Brands and D. Chaum, "Distance-bounding protocols," in *USENIX Security Symposium*, 1994.

[48] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in *Proceedings of the second ACM conference on Wireless network security*, 2009.

[49] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *IEEE International Conference on Communications*, 2010.

[50] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[51] S. Oh and M. Gruteser, "Multi-node coordinated jamming for location privacy protection," in *Proceedings of the Robotics: Science and Systems Conference*, 2011.

[52] J. H. Halton, "Sigma-algebra theorems," *Monte Carlo Methods and Applications*, vol. 14, no. 2, pp. 171–189, 2008.

[53] J. A. Gubner, *Probability and random processes for electrical and computer engineers*. Cambridge, United Kingdom: Cambridge University Press, pp. 17–22, 2006.

[54] E. Chew, M. Swanson, K. M. Stine, N. Bartol, A. Brown, and W. Robinson, "Sp 800-55 rev. 1. performance measurement guide for information security," 2008.