Bluetooth MAC Spoofing System

Anonymous CVPR submission

Paper ID ****

Abstract

1. Introduction

2. How to measure *speed* using two BMS

We know that speed is

$$speed = \frac{\text{distance covered}}{\text{time taken}} \tag{1}$$

From Figure [1] it can be seen that distance covered $=$ distance between point A & point B whereas time taken $=$ time taken to travel from point A to point B. By putting the values of **distance covered** and **time taken** from Figure[1] in equation[1] we get

$$speed = \frac{\hat{d} - R_2 + R_1}{(\hat{t_2} - T_2) - (\hat{t_1} - T_1)} \tag{2}$$

whereas, $\hat{d}$ is distance between two sites. R_1 & R_2 is range of site 1 and site 2, respectively. $\hat{t_1}$ & $\hat{t_2}$ is Timestamp of detection of first packet at site 1 and site 2, respectively. T_1 & T_2 is time till first detection after entering into the range of site 1 and site 2, respectively.

For a single pass of a vehicle from site 1 to site 2, $\hat{d}$, $\hat{t_1}$ and $\hat{t_2}$ are constants. Whereas, R_1, R_2, and T_1, T_2 are random variables. Hence we need to compute the Expected value of speed.

$$E[speed] = E\left[\frac{\hat{d} - R_2 + R_1}{(\hat{t_2} - T_2) - (\hat{t_1} - T_1)}\right] \tag{3}$$

$$var[speed] = var\left[\frac{\hat{d} - R_2 + R_1}{(\hat{t_2} - T_2) - (\hat{t_1} - T_1)}\right] \tag{4}$$

Equation [5] and [6] can be written as

$$E[Z] = E\left[\frac{X}{Y}\right]$$

and

$$var[Z] = var\left[\frac{X}{Y}\right]$$

whereas $X = \hat{d} - R_2 + R_1$, $Y = (\hat{t_2} - T_2) - (\hat{t_1} - T_1)$ and $Z = speed$.

2.1. Computing $E[Z]$ and $var[Z]$

If random variable Y is an arbitrary non-linear function of two random variables X_1, X_2

$$Y = g(X_1, X_2) \tag{5}$$

then Taylor Series Expansion of Y around mean, μ_1, μ_2 will be [1]

$$\begin{aligned} Y &= g(\mu_1, \mu_2) \\ &+ (X_1 - \mu_1)\frac{\mathrm{d}g}{\mathrm{d}X_1}\bigg|_{\mu_1,\mu_2} + (X_2 - \mu_2)\frac{\mathrm{d}g}{\mathrm{d}X_2}\bigg|_{\mu_1,\mu_2} + \\ &+ \frac{(X_1 - \mu_1)^2}{2!}\frac{\mathrm{d}^2 g}{\mathrm{d}X_1^2}\bigg|_{\mu_1,\mu_2} + \frac{(X_2 - \mu_2)^2}{2!}\frac{\mathrm{d}^2 g}{\mathrm{d}X_2^2}\bigg|_{\mu_1,\mu_2} \\ &+ (X_1 - \mu_1)(X_2 - \mu_2)\frac{\partial^2 g}{\partial X_1 \partial X_2}\bigg|_{\mu_1,\mu_2} + \ldots \end{aligned} \tag{6}$$

If, $g(X, Y) = \frac{X}{Y}$ then,

$$\begin{aligned} g(X, Y) &= \frac{\mu_X}{\mu_Y} + \frac{1}{\mu_Y}(X - \mu_X) - \frac{\mu_X}{\mu_Y^2}(Y - \mu_Y) \\ &+ \frac{\mu_X}{\mu_Y^3}(Y - \mu_Y)^2 - \frac{1}{\mu_Y^2}(X - \mu_X)(Y - \mu_Y) + \ldots \end{aligned} \tag{7}$$

Second order approximation of $E[g(X, Y)]$ and first-order approximation of $var[g(X, Y)]$ is [1],

$$E\left[\frac{X}{Y}\right] \approx \frac{\mu_X}{\mu_Y} + \frac{\mu_X}{\mu_Y^3}var[Y] - \frac{1}{\mu_Y^2}cov[X, Y] \tag{8a}$$

$$var\left[\frac{X}{Y}\right] \approx \frac{var[X]}{\mu_Y^2} - \frac{2\mu_X}{\mu_Y^3}cov[X, Y] + \frac{\mu_X^2}{\mu_Y^4}var[Y] \tag{8b}$$

$$E[X] = \hat{d} - E[R_2] + E[R_1] \tag{9a}$$
$$E[Y] = (\hat{t_2} - \hat{t_1}) - (E[T_2] - E[T_1]) \tag{9b}$$
$$var[X] = var[R_1] + var[R_2] \tag{9c}$$
$$var[Y] = var[T_1] + var[T_2] \tag{9d}$$
$$cov[X,Y] = cov[R_1,T_1] + cov[R_2,T_2] \tag{9e}$$

since $\hat{d}$, $\hat{t_1}$ and $\hat{t_2}$ are constants, $var[X] = var[-X]$, R_1 & R_2 are independent, both sites are well seperated so T_1 & T_2 are independent, R_1, T_2 and R_2, T_1 are independent.

2.2. Computing $COV[RANGE, TTDD]$

Assumption: *Range* and *Time Till Device Discovery* are independent. Hence $cov[range, ttdd] = 0$.

2.3. Range

Range of a site is a function of antenna-type and enviornment of a particular site. More specifically [3],

$$\frac{P_r}{P_t} = \left(\frac{\lambda \sqrt[2]{G_l}}{4\pi d}\right)^{\gamma} \tag{10}$$

γ is the enviornment factor (2 for Free-Space[3], 2.4 in our-testing-enviornment), λ is wavelength (0.125m for 2.4GHz), G_l depends on directionality of antenna (1 for Omni-directional antenna[3]), P_r is received power in watts (1×10^{-12} for -80dBm), P_t is transmitted power in watts (3×10^{-3} for 5dBm), d is distance between two antennas (corresponds to range for P_r = -90dBm).
For above mention values of variables, the range of antenna turn out to be $\sim 88m$.

2.4. Time Till Device Detection

TTDD of a site is a function of *time taken by bluetooth protocol to detect a slave device in ideal communiation enviornment* and *number of retires due to noise and packet loss*.

$$\begin{aligned} \text{T} &= \textit{number of tries} \\ &\quad \times \textit{time till master and slave's frequencies match} \end{aligned} \tag{11}$$

We are going to model *packet loss* with *Geometric Distribution with infinite tries and parameter p*, $E[\textit{number of tries}] = \frac{1}{p}$ whereas p is the *probability of an error-free packet transmission from source to destination*. Whereas, *time till master and slave's frequencies match* is modeled by a **variant** of [2]. Note that *packet loss* and *time till frequencies match* are both independent variables. So their expected value is the product of their respective expected values.

2.5. Extending $speed$ estimator to mth and nth detections

From Figure [2] it can be seen that previously build estimator of $speed$ for first-to-first detection can be extended to mth detection of site 1 and nth detection of site 2. Putting values from Figure[2] in equation[1] we get

$$speed_{mn} = \frac{\hat{d} - R_2 + R_1}{(\hat{t}_{2n} - \hat{t}_{1m}) - (nT_2 - mT_1)} \tag{12}$$

$$E[distance] = \hat{d} - E[R_2] + E[R_1] \tag{13a}$$
$$E[time] = (\hat{t}_{2n} - \hat{t}_{1m}) - (nE[T_2] - mE[T_1]) \tag{13b}$$
$$var[distance] = var[R_1] + var[R_2] \tag{13c}$$
$$var[time] = m^2 \times var[T_1] + n^2 \times var[T_2] \tag{13d}$$
$$var[T] = var[p]var[TTFM] \tag{13e}$$
$$+ var[p]E[TTFM]^2 + var[TTFM]E[p]^2 \tag{13f}$$
$$\tag{13g}$$
$$cov[distance, time] = 0, Assumption \tag{13h}$$

3. Factors affecting $speed$ estimation

3.1. Time till frequencies match

If *time till master and slave's frequencies match* is zero i.e. devices get detected as soon as they enter the antenna range of a device then $E[TTFM] = var[TTFM] = var[T] = 0$. From 13e, 13d and 8b, $var[speed]$ decreases. Even if $E[TTFM] \neq 0$ and only $var[TTFM] = 0$ even then $var[speed]$ decreses.

3.2. Packet Loss

If $P(packet - loss) = fixed$, there is no change in *probability of packet loss*, then $var[T]$ decreases. From 13e, 13d and 8b, $var[speed]$ decreases.

3.3. Range of site

If range of a site is fixed i.e. there is no change in range of antenna due to any external and internal factors, then $E[Range] = constand$ and $var[Range] = 0$. From 13c and 8b, $var[speed]$ decreases.

3.4. Choice of m & n for speed calculation

3.5. Distance between sites

References

[1] H. Benaroya and S. M. Han. *Probability Models in Engineering and Science*. CRC Press, Taylor and Francis Group, 2005.

Refer to page 168 for derivation of mean and variance of a general function of N RVs. 1

[2] G. Chakraborty, K. Naik, D. Chakraborty, N. Shiratori, and D. Wei. Analysis of the bluetooth device discovery protocol. *Wireless Networks*, 16(2):421–436, 2010. 2

[3] A. Goldsmith. *Wireless Communications*. Cambridge University Press, 2005. Refer to page 28 for Free-Space path losses. 2