Time-based Countermeasures for Relay Attacks on PKES Systems

Yifan Xie, Hyung June Kim, Sa Yong Chong and Taek Lyul Song
Department of Electronic Systems Engineering, Hanyang University, Ansan, Republic of Korea

Keywords: PKES, Relay Attack, Distance Bounding, TOA, Localization.

Abstract: The development of passive keyless entry and start (PKES) systems in modern vehicles enables drivers to access and control their vehicles remotely using smart keys, which improves the driving conveniences. The PKES system verifies the smart key identity if the communication channel between the vehicle and the smart key is established. When the message in the communication channel is relayed by other devices, it can be manipulated by the attackers and the PKES systems become vulnerable. The distance bounding protocol, which estimates the physical proximity between the vehicle and the smart key, is one of the countermeasures against relay attacks. In this paper, the time-based distance bounding is studied. Since the effectiveness of distance bounding protocol relies heavily on the estimation accuracy, various time-based estimation algorithms are enumerated and compared in this paper.

1 INTRODUCTION

Traditional vehicles are usually accessed and authorized to drive through physical keys and locking systems. In order to improve drivers' experience and convenience, modern vehicles are embedded with passive keyless entry and start (PKES) systems, which allows the driver to open the door and start the engine remotely by pressing the button on the smart key (Francillon et al., 2011; Ahmad et al., 2018; Patel et al., 2018).

However, the PKES systems are vulnerable if the messages between the vehicle and the smart key are relayed by some attack devices. When the attacker places one attack device near the vehicle, fake signals are seduced from the vehicle and sent to the smart key to get *open*/*start* authorizations. Another attack device is then placed a few meters from the smart key to establish the relay channel. The signals from the vehicle are received by the attack device instead of the smart key such that the messages are relayed and can be manipulated. The possibility of the relay attack is caused by the PKES system vulnerability. In a PKES system, the vehicle periodically probes the communication channel to search the short beacons from the smart key. Once the short beacon is detected by the vehicle, i.e. the smart key is located inside the vehicle's communication range, the PKES system concludes that the smart key is in the proximity of the vehicle and all commands from the smart key are authorized. This verification procedure assumes that the communication ability implies the physical proximity, which makes the relay attacks possible.

Numerous countermeasures are proposed in past decades to prevent the relay attacks on PKES systems (Francillon et al., 2011). For instances, (1) the smart key can be put into a protective cage (made by metallic) for signal shielding after parking the vehicle; (2) design another button on the smart key to disable the embedded battery after parking the vehicle; (3) use the distance bounding protocol to estimate the physical proximity, etc. The first two countermeasures are inconvenient and the vehicle could still be under the relay attacks when the driver forgets to take actions. The distance bounding based countermeasure is recommended and studied in this paper. The distance bounding protocol provides protections against attacks on access control systems by verifying the smart key location. The command from the smart key will be authorized only if when it is transmitted from the physical proximity of the vehicle. Therefore, the accuracy of the estimated smart key location is critical for the distance bounding protocol.

Among all distance bounding protocols, the smart key location can be estimated by diverse methods according to signal properties of phase change, amplitude attenuation and traveling time, etc (Ranganathan and Capkun, 2017). The signal traveling time information can be exploited by the time of arrival (TOA) measurement and the time difference of ar-

Xie, Y., Kim, H., Chong, S. and Song, T.
Time-based Countermeasures for Relay Attacks on PKES Systems.
DOI: 10.5220/0007957407950801
In *Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2019)*, pages 795-801
ISBN: 978-989-758-380-3

rival (TDOA) measurement. The TOA measurement has smaller sensor noise relative to the TDOA measurement, which leads to its popularity. In this paper, two least-square (LS) based methods called unconstrained squared-range-based LS (USR-LS) and constrained squared-range-based LS (CSR-LS) are introduced for position estimation using the TOA measurements. Both the USR-LS method and the CSR-LS method minimize the residual using only one set of the TOA measurements. Since the effectiveness of the TOA-based countermeasure relies on estimation accuracy, the authors propose to improve the estimation accuracy by using multiple TOA measurement sets. The first TOA measurement set is used for track initialization via the CSR-LS method and the other TOA measurement sets are used serially by an extended Kalman filter (EKF).

The rest of the paper is organized as follows. The relay attack model and the distance bounding are introduced in Section 2. Analyses for the TOA and the TDOA measurement selection are discussed in Section 3. Details for the USR-LS method, the CSR-LS method and the multiple-transmission method are described in Section 4. Simulations for the three methods are studied in Section 5, followed by the conclusions in Section 6.

2 PROBLEM STATEMENTS

2.1 Relay Attack Model

The PKES system in modern vehicles verifies whether the correct smart key is located around the vehicle by verifying the communication ability, assuming that the communication ability implies the physical proximity. This verifying procedure makes the PKES system vulnerable to the relay attacks. In typical relay attacks, two attack devices are deployed near the vehicle and the smart key separately to establish the communication channel for relayed messages as shown in Fig. 1.

When the driver parks his vehicle and leaves the parking lot, the attacker approaches the door handle with the first attack device to seduce a fake signal to the smart key. The second attack device is deployed near the exit of the parking lot. When driver passes the exit with smart key inside his pocket, the second attack device instead of the key receives the signal from the vehicle and sends the *open* command to the vehicle. Consequently the attacker succeeds to enter the vehicle. Similar fake signals are created when the attacker starts the engine button to seduce a fake *start* command. This relay attack model enables the attacker to steal even the smart key is physically remote from the vehicle (Francillon et al., 2011).

2.2 Distance Bounding

For the purpose of preventing the relay attacks on PKES systems, the distance bounding protocol (Brands and Chaum, 1993) is proposed to measure the upper-bound distance (physical proximity) between the verifier (the smart key) and the prover (the vehicle). Various distance bounding protocols are proposed in recent years, emphasizing aspects such as location privacy, provable security, noise channels, nonce space size, etc (Rasmussen and Čapkun, 2008; Boureanu et al., 2013; Hancke and Kuhn, 2005; Mitrokotsa et al., 2013).

Apart from the distance bounding protocol types, methods for estimating the physical distance between the verifier and the prover can be classified into various categories regarding to measurement types: (1) phase of radio frequency signal; (2) received signal strength (RSS); (3) signal arrival time, etc (Ranganathan and Capkun, 2017).

When the signal arrival time in each sensor is available, both the TOA measurement and the TDOA measurement can be generated that there exists two options for estimating the physical distance. In order to select a more appropriate measurement type for the distance bounding protocol, analyses including the superiorities and the defects of the TDOA and the TOA based localization methods are discussed in Section 3.

2.3 State Vector and Distance Measurement

Assume that N time-synchronized sensors are mounted on the vehicle at predetermined positions $\mathbf{x}_i = [x_i, y_i]^T \ (i = 1, ..., N)$ and passively receive the signals transmitted from the smart key. The smart key at position $\mathbf{x} = [x, y]^T$ not only broadcasts the acknowledgement (ACK) request to the PKES system but also the time-stamp of the signal transmitting time. The TOA measurements can be obtained by subtracting the signal transmitting time and receiving time measured by each sensor. The radius vector from sensor s_i to the smart key is denoted by $\mathbf{r}_i = \mathbf{x} - \mathbf{x}_i$. By multiplying with the signal propagation speed c, the TOA measurement in sensor s_i can be converted into the range measurement

$$z_i = ||\mathbf{r}_i|| + \nu_i = h_i(\mathbf{x}_i) + \nu_i, \ i = 1, ..., N \qquad (1)$$

where $\nu_i \sim \mathcal{N}\left(0, \sigma^2\right)$ is the range measurement noise.

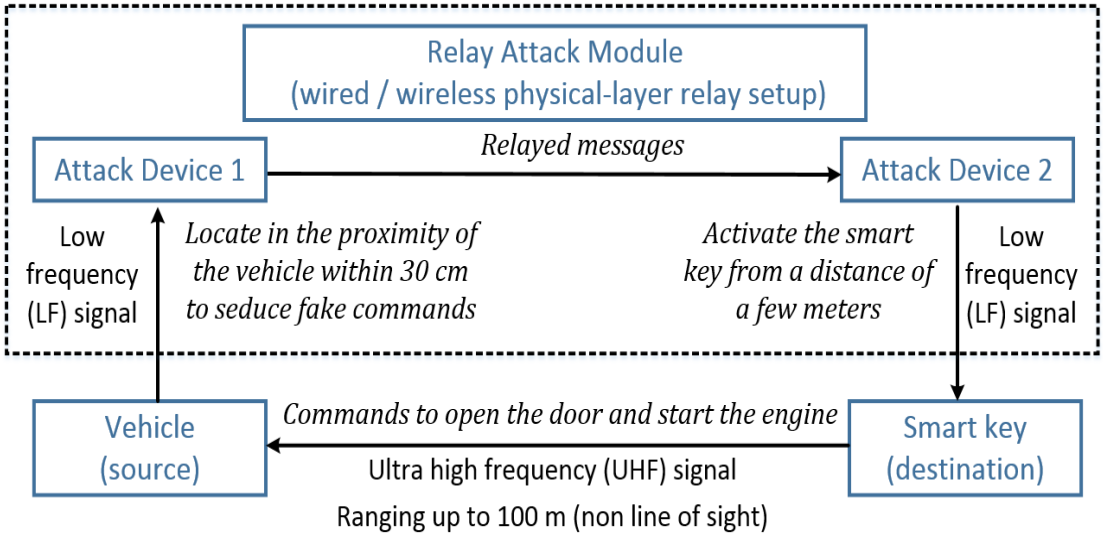

Figure 1: An example of relay attacks on PKES systems.

Let sensor s_N be the common reference sensor in the sensor network, the TDOA measurements in range domain are given by

$$\begin{aligned} z_{i,N} &= (||\mathbf{r}_i|| - ||\mathbf{r}_N||) + (\nu_i - \nu_N) \\ &= h_i(\mathbf{x}_i) - h_N(\mathbf{x}_N) + u_{i,N},\ i = 1,...,N-1 \end{aligned} \quad (2)$$

where $u_{i,N} \sim \mathcal{N}(0, 2\sigma^2)$ is the range difference measurement noise.

3 TIME-BASED MEASUREMENT ANALYSIS

The superiority of the TDOA based localization method (Gillette and Silverman, 2008; Ho and Chan, 1993) is that the clocks only need to synchronize with the reference clock instead of the entire sensor network. But the TDOA based methods inevitably suffer from localization inaccuracy. A comparison between the measurement noises of TOA and TDOA by eqs (1) and (2) suggests that the covariance of TDOA is two times bigger than that of TOA. This can also be numerically analyzed by comparing the measurement uncertainty coverages of TOA and TDOA. The measurement uncertainty coverage indicates an area where the target can be at an arbitrary position inside, which can be evaluated by the inverse of Fisher information matrix (FIM) (Bar-Shalom et al., 2004; Bar-Shalom et al., 2011)

$$\mathbf{P}_k = \left(\mathbf{H}_k^T \mathbf{R}_k \mathbf{H}_k\right)^{-1}, \quad (3)$$

where $\mathbf{H}_k$ is the Jacobian matrix and $\mathbf{R}_k$ is the measurement noise covariance matrix. For TOA-based methods, the Jacobian matrix and measurement noise covariance matrix are given by

$$\mathbf{H}_k^{TOA} = \begin{bmatrix} \frac{\partial h_1(\mathbf{x}_1)}{\mathbf{x}_1} \\ \vdots \\ \frac{\partial h_N(\mathbf{x}_N)}{\mathbf{x}_N} \end{bmatrix} = \begin{bmatrix} \frac{\mathbf{r}_1}{||\mathbf{r}_1||} \\ \vdots \\ \frac{\mathbf{r}_N}{||\mathbf{r}_N||} \end{bmatrix}, \quad (4)$$

$$\mathbf{R}_k^{TOA} = \sigma^2 \mathbf{I}_N, \quad (5)$$

where $\mathbf{I}_n$ indicates an $n \times n$ identity matrix. Similarly, the Jacobian matrix and measurement noise covariance matrix for TDOA based methods are given by (Kaune et al., 2011; Xie et al., 2018)

$$\mathbf{H}_k^{TDOA} = \begin{bmatrix} \frac{\partial h_1(\mathbf{x}_1)}{\mathbf{x}_1} - \frac{\partial h_N(\mathbf{x}_N)}{\mathbf{x}_N} \\ \vdots \\ \frac{\partial h_N(\mathbf{x}_{N-1})}{\mathbf{x}_{N-1}} - \frac{\partial h_N(\mathbf{x}_N)}{\mathbf{x}_N} \end{bmatrix} = \begin{bmatrix} \frac{\mathbf{r}_1}{||\mathbf{r}_1||} - \frac{\mathbf{r}_N}{||\mathbf{r}_N||} \\ \vdots \\ \frac{\mathbf{r}_{N-1}}{||\mathbf{r}_{N-1}||} - \frac{\mathbf{r}_N}{||\mathbf{r}_N||} \end{bmatrix}, \quad (6)$$

$$\mathbf{R}_k^{TDOA} = 2\sigma^2 \begin{bmatrix} 1 & 0.5 & \cdots & 0.5 \\ 0.5 & 1 & \cdots & 0.5 \\ \vdots & \vdots & \ddots & \vdots \\ 0.5 & 0.5 & \cdots & 1 \end{bmatrix}_{(N-1)\times(N-1)}. \quad (7)$$

Given a situation where $N = 6$ sensors are mounted on a vehicle and the smart key transmits the UHF signal 5 m away from the vehicle center(sensor s_3 position), the measurement uncertainty coverages for both TOA and TDOA are illustrated in Fig. 2. The measurement uncertainty coverage of TDOA is significantly larger than that of TOA and even larger the vehicle size, which suggests the inappropriateness of using the TDOA measurement for distance bounding protocol.

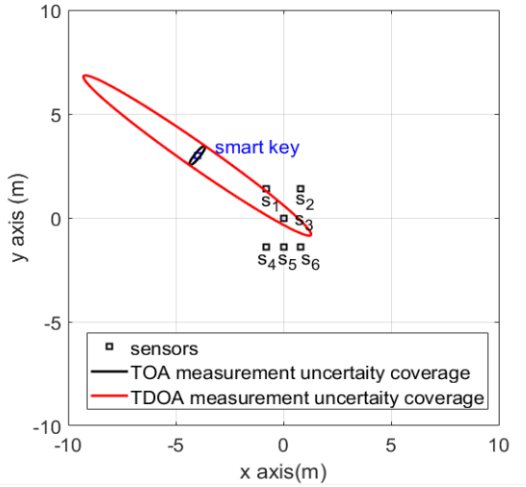

Figure 2: An example of measurement uncertainty coverage comparison($\sigma = 0.3\ m$).

Another problem of constraining the TDOA measurement for distance bounding protocol is that the sensors are closely spaced. The standard hyperbola equation indicating the transmitter position for a TDOA measurement is given by

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1, \tag{8}$$

which subjects to constraints of $c^2 = a^2 + b^2$ and $c > a$. The distance between sensor s_1 and sensor s_2 is $2c = 1.6\ m$ in Fig. 2, and the corresponding TDOA measurement is $2a = 1.48\ m$. Since the sensors are not perfect, the TDOA measurement is usually corrupted by the sensor noise with a standard deviation $\sqrt{2}\sigma$. Therefore the noise-corrupted TDOA measurement is $(2a + \sqrt{2}\sigma) \approx 1.9\ m > 2c$, which violates the hyperbola constraint. The TDOA based localization algorithms cannot be applied under such circumstances, otherwise an inaccurate result can be expected.

Therefore the TOA measurement is studied in this paper. Various TOA based localization methods are discussed detailedly in the following sections.

4 TOA-BASED ESTIMATION

The least square approach has been widely studied in the TOA measurement-based target localization (Smith and Abel, 1987; Cheung et al., 2004a; Cheung et al., 2004b; Cheung and So, 2005; Stoica and Li, 2006; Beck et al., 2008). The methods in (Smith and Abel, 1987; Stoica and Li, 2006) provide a simple but efficient solution by neglecting the quadratic constraint, which is called unconstrained squared-range-based LS estimate. The constrained squared-range-based LS estimate in (Beck et al., 2008) improves the localization accuracy by introducing a Lagrange multiplier and the solution is obtained through a bisection algorithm, which makes it computationally expensive. Both the USR-LS method and the CSR-LS method require only one set of TOA measurements. The proposed multiple-transmission method require the vehicle owner pressing the smart key multiple times such that multiple sets of TOA measurements are generated and used for improving the estimation accuracy. Detailed descriptions for the above methods are presented in the following.

4.1 USR-LS Method

The essence of least square is to estimate the optimal smart key position by minimizing the residual

$$\begin{aligned} & min \sum_{i=1}^{N} \left(||\mathbf{x} - \mathbf{x}_i||^2 - z_i^2 \right)^2 \\ = \ & min \sum_{i=1}^{N} \left[(x - x_i)^2 + (y - y_i)^2 - z_i^2 \right]^2 \\ = \ & min \sum_{i=1}^{N} \left(-2x_i x - 2y_i y + x^2 + y^2 + x_i^2 + y_i^2 - z_i^2 \right)^2, \end{aligned} \tag{9}$$

which can be expressed by a matrix form as

$$L(\boldsymbol{\omega}) = (\mathbf{A}\boldsymbol{\omega} - \mathbf{b})^T (\mathbf{A}\boldsymbol{\omega} - \mathbf{b}), \tag{10}$$

where

$$\mathbf{A} = \begin{bmatrix} -2x_1 & -2y_1 & 1 \\ \vdots & \vdots & \vdots \\ -2x_N & -2y_N & 1 \end{bmatrix}, \boldsymbol{\omega} = \begin{bmatrix} x \\ y \\ x^2 + y^2 \end{bmatrix}, \tag{11}$$

$$\mathbf{b} = \begin{bmatrix} z_1^2 - (x_1^2 + y_1^2) \\ \vdots \\ z_N^2 - (x_N^2 + y_N^2) \end{bmatrix}. \tag{12}$$

The solution of $L(\boldsymbol{\omega})$ can be obtained by

$$\frac{\partial L(\boldsymbol{\omega})}{\partial \boldsymbol{\omega}} = 2\mathbf{A}^T\mathbf{A}\boldsymbol{\omega} - 2\mathbf{A}^T\mathbf{b} = 0, \tag{13}$$

and the corresponding optimal solution is

$$\hat{\boldsymbol{\omega}} = \left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T\mathbf{b}. \tag{14}$$

The solution $\hat{\boldsymbol{\omega}}$ does not follow the quadratic constraint. For instance, the estimated variable vector for Fig. 2 is

$$\hat{\boldsymbol{\omega}} = \begin{bmatrix} -3.99 \\ 3.78 \\ 25.67 \end{bmatrix}, \tag{15}$$

where $(-3.99)^2 + (3.78)^2 = 30.21 \neq 25.67$ and fails to follow the quadratic constraint.

4.2 CSR-LS Method

The CSR-LS method minimizes the quadratic function in eq (10) subjecting to a quadratic constraint such that

$$L(\omega) = \{(\mathbf{A}\omega - \mathbf{b})^T(\mathbf{A}\omega - \mathbf{b}) : ||\mathbf{x}||^2 = x^2 + y^2\}, \tag{16}$$

which is equivalent to minimize the Lagrangian

$$L(\omega, \lambda) = (\mathbf{A}\omega - \mathbf{b})^T(\mathbf{A}\omega - \mathbf{b}) + \lambda(2\mathbf{f}^T\omega + \omega^T\mathbf{D}\omega), \tag{17}$$

where

$$\mathbf{f} = \begin{bmatrix} 0 \\ 0 \\ -0.5 \end{bmatrix}, \mathbf{D} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \tag{18}$$

and λ is the Lagrange multiplier.

Similarly, the solution of $L(\omega, \lambda)$ can be obtained by

$$\frac{\partial L(\omega, \lambda)}{\partial \omega} = 2(\mathbf{A}^T\mathbf{A} + \lambda\mathbf{D})\omega - 2\mathbf{A}^T\mathbf{b} + 2\lambda\mathbf{f} = 0, \tag{19}$$

and the corresponding solution is

$$\hat{\omega}(\lambda) = (\mathbf{A}^T\mathbf{A} + \lambda\mathbf{D})^{-1}(\mathbf{A}^T\mathbf{b} - \lambda\mathbf{f}). \tag{20}$$

The solution $\hat{\omega}(\lambda)$ subjects to the quadratic constraint

$$\phi(\lambda) \equiv 2\mathbf{f}^T\hat{\omega}(\lambda) + \hat{\omega}(\lambda)^T\mathbf{D}\hat{\omega}(\lambda) = 0. \tag{21}$$

The method in (Cheung et al., 2004b) manipulates eq (21) and transforms it into a five-root equation, and λ is determined by a complicated root finding procedure.

The optimization in eq (16) leads to a nonconvex problem. There exists multiple local optima such that a global optimum can be hardly obtained. The method in (Beck et al., 2008) provides an efficiently and globally optimal solution by converting it into a generalized trust region subproblem (GTRS) (Moré, 1993). According to GTRS, function $\phi(\lambda)$ is strictly decreasing over interval

$$I_{PD} = \left(-\frac{1}{\lambda_1(\mathbf{D}, \mathbf{A}^T\mathbf{A})}, \infty\right), \tag{22}$$

where $\lambda_i(\mathbf{E}, \mathbf{F}) = \lambda_i(\mathbf{F}^{-1/2}\mathbf{E}\mathbf{F}^{-1/2})$ indicates the ith eigenvalue of $\mathbf{F}^{-1/2}\mathbf{E}\mathbf{F}^{-1/2}$ (ordered increasingly). Therefore the solution for eq (21) can be obtained by applying a bisection algorithm over interval I_{PD} instead of applying the complicated root finding procedure. More details for the CSR-LS method are available in (Beck et al., 2008).

4.3 Multiple-transmission Method

The smart key in PKES systems is powered by an embedded battery. In order to save the energy consumption as well as prolong the service time of the battery, the vehicle owner is recommended to press the smart key only once to activate the PKES system. The USR-LS method and the CSR-LS method are designated to optimize the estimation accuracy under the assumption of single signal transmission. For situations where the estimation accuracy dominates the evaluation criteria, multiple signal transmissions from the smart key contribute to improving the estimation accuracy since more information is accumulated. In these cases, the vehicle owner is recommended to press the smart key M $(M > 1)$ times. Each transmission generates a set of TOA measurements and all TOA measurement sets are mutually uncorrelated and independent. The method for handling the multiple signal transmissions is proposed and summarized in the following:

1) The first TOA measurement set is used for the CSR-LS method to obtained the state mean of an initial track $\hat{\mathbf{x}}$. The FIM is calculated to obtain the state covariance of the initial track $\hat{\mathbf{P}}$.
2) The other $(M-1)$ TOA measurement sets are used by EKF to serially update the track state $\hat{\mathbf{x}}$ and $\hat{\mathbf{P}}$.

The TOA measurement generated by the jth sensor in the ith transmission is denoted as z_j^i. The pseudo code for the serial EKF update is shown in Algorithm 1.

Algorithm 1: Serial EKF update.

```
for i = 2 : M do
  for j = 1 : N do
    x̄ = x̂, P̄ = P̂
    H_j = ∂h_j(x̄)/∂x̄
    S_j = H_j P̄ H_j^T + σ^2
    K_j = P̄ H_j^T S_j^{-1}
    x̂ = x̄ + K_j(z_j^i − h_j(x̄))
    P̂ = P̄ − K_j H_j P̄
  end for
end for
```

5 SIMULATION

The simulation settings of the sensor deployment and sensor noise are identical to that of in Fig. 2, where $N = 6$ sensors are mounted on the vehicle and the smart key is located 5 m from the vehicle center. The

standard deviation of the TOA measurement noise is $\sigma = 0.3$ m. The simulation includes 100 Monte Carlo trials. In each trial, the USR-LS method, the CSR-LS method and the multiple-transmission method (with $M = 2$) are all applied to estimate the smart key position. The estimation accuracy is evaluated by root mean square error (RMSE). In order to achieve a more intuitive simulation result, the RMSE at every position of the surveillance area is calculated. The simulation results are shown in Figs. 3-5. As can be seen that the numerical results are presented by RMSE distributions in which detailed RMSE values are distinguished by a color bar.

The smart key locates at position $[-4,3]^T$. The corresponding RMSE values for USR-LS, CSR-LS and multiple-transmission are 1.11 m, 0.6331 m and 0.4348 m, respectively. The multiple-transmission method delivers the most accurate estimation at the costs of higher computational load and more energy consumption. A summary for the three estimation methods are listed in Table 1. According to Table 1, the comparison between the USR-LS method and the CSR-LS method indicates a trade-off between the computational load and estimation accuracy. The comparison between the CSR-LS method and the multiple-transmission method indicates a trade-off between energy consumption and estimation accuracy.

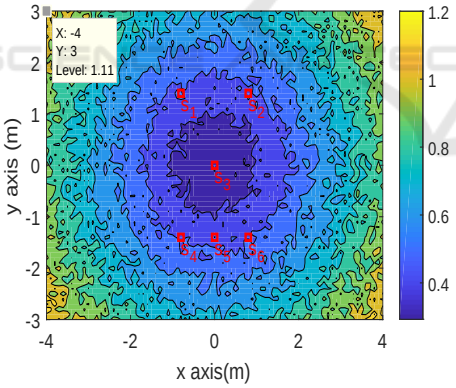

Figure 3: RMSE distribution of the USR-LS method.

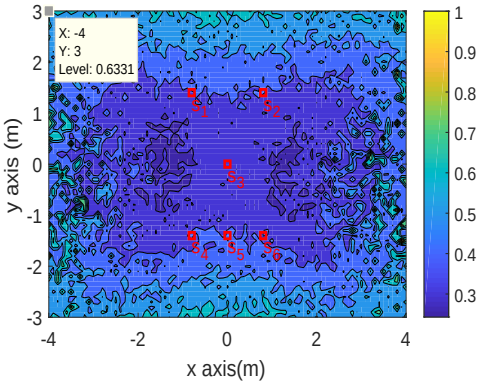

Figure 4: RMSE distribution of the CSR-LS method.

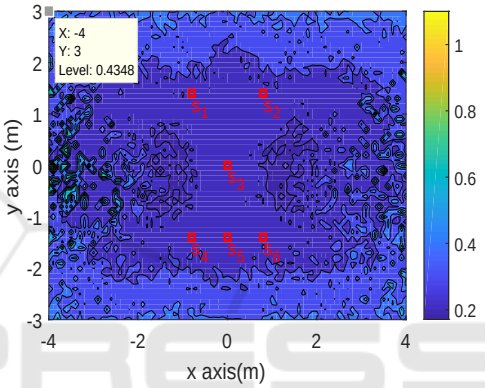

Figure 5: RMSE distribution of the multiple-transmission method.

6 CONCLUSION

The distance bounding protocol was proposed to protect PKES systems from the relay attacks by estimating the physical distance between the vehicle and the smart key. The effectiveness of distance bounding protocol relies heavily on the estimation accuracy. In this paper, three TOA based position estimation methods such as USR-LS, CSR-LS and multiple-transmission are reviewed and proposed to validate the estimation accuracy. Simulation results show that trade-offs can be made among computational load, estimation accuracy and energy consumption when different methods are applied. Additionally hybrid schemes that use combinations of the discussed methods enable the PKES system to operate more flexibly under diverse environmental conditions will be explored in future studies.

ACKNOWLEDGEMENT

This work was supported by Hanwha Systems Company under the contract U-17-017.

REFERENCES

Ahmad, U., Song, H., Bilal, A., Alazab, M., and Jolfaei, A. (2018). Secure passive keyless entry and start system using machine learning. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pages 304–313.

Table 1: TOA-based estimation summary.

Method	Computational load	Estimation accuracy	Energy consumption
USR-LS	low	low	low
CSR-LS	medium	medium	low
Multiple-transmission	high	high	high

Bar-Shalom, Y., Li, X. R., and Kirubarajan, T. (2004). *Estimation with applications to tracking and navigation: theory algorithms and software*. John Wiley & Sons.

Bar-Shalom, Y., Willett, P. K., and Tian, X. (2011). *Tracking and data fusion*. YBS publishing.

Beck, A., Stoica, P., and Li, J. (2008). Exact and approximate solutions of source localization problems. *IEEE Transactions on signal processing*, 56(5):1770–1778.

Boureanu, I., Mitrokotsa, A., and Vaudenay, S. (2013). Secure and lightweight distance-bounding. In *International Workshop on Lightweight Cryptography for Security and Privacy*, pages 97–113. Springer.

Brands, S. and Chaum, D. (1993). Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer.

Cheung, K. W., Ma, W.-K., and So, H.-C. (2004a). Accurate approximation algorithm for toa-based maximum likelihood mobile location using semidefinite programming. In *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 2, pages ii–145. IEEE.

Cheung, K. W. and So, H.-C. (2005). A multidimensional scaling framework for mobile location using time-of-arrival measurements. *IEEE transactions on signal processing*, 53(2):460–470.

Cheung, K. W., So, H.-C., Ma, W.-K., and Chan, Y.-T. (2004b). Least squares algorithms for time-of-arrival-based mobile location. *IEEE Transactions on Signal Processing*, 52(4):1121–1130.

Francillon, A., Danev, B., and Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

Gillette, M. D. and Silverman, H. F. (2008). A linear closed-form algorithm for source localization from time-differences of arrival. *IEEE Signal Processing Letters*, 15:1–4.

Hancke, G. P. and Kuhn, M. G. (2005). An rfid distance bounding protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 67–73. IEEE.

Ho, K. and Chan, Y. (1993). Solution and performance analysis of geolocation by TDOA. *IEEE Transactions on Aerospace and Electronic Systems*, 29(4):1311–1322.

Kaune, R., Hörst, J., and Koch, W. (2011). Accuracy analysis for TDOA localization in sensor networks. In *Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on*, pages 1–8. IEEE.

Mitrokotsa, A., Peris-Lopez, P., Dimitrakakis, C., and Vaudenay, S. (2013). On selecting the nonce length in distance-bounding protocols. *The Computer Journal*, 56(10):1216–1227.

Moré, J. J. (1993). Generalizations of the trust region problem. *Optimization methods and Software*, 2(3-4):189–209.

Patel, J., Das, M. L., and Nandi, S. (2018). On the security of remote key less entry for vehicles. In *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6.

Ranganathan, A. and Capkun, S. (2017). Are we really close? verifying proximity in wireless systems. *IEEE Security & Privacy*.

Rasmussen, K. B. and Čapkun, S. (2008). Location privacy of distance bounding protocols. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 149–160. ACM.

Smith, J. and Abel, J. (1987). Closed-form least-squares source location estimation from range-difference measurements. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 35(12):1661–1669.

Stoica, P. and Li, J. (2006). Lecture notes-source localization from range-difference measurements. *IEEE Signal Processing Magazine*, 23(6):63–66.

Xie, Y., Lee, J. H., and Song, T. L. (2018). Analysis for reference sensor selection in time difference of arrival-based localisation. *Electronics Letters*, 54(25):1454–1456.