Side-Channel Security on Key Exchange Protocol: Timing and Relay Attacks

Mohd Anuar Mat Isa, Habibah Hashim, Syed Farid Syed Adnan, Nur Nabila Mohamed, Yasin Fitri Alias
Faculty of Electrical Engineering, 40450 UiTM Shah Alam, Selangor, Malaysia

Article Info

Article history:

Received Feb 1, 2018
Revised Apr 21, 2018
Accepted Apr 27, 2018

Keywords:

Side-channel attack
Timing
Relay
Key exchange protocol
Diffie-hellman

ABSTRACT

The advancing of Key Exchange Protocol (KEP) is compulsory to secure the connected world via Internet of Thing (IoT), cryptocurrency and blockchain, virtual intelligent, smart computing etc. To address the security issues in the Internet based computing systems, this paper explores the side-channel security for KEP, namely timing and relay attacks. Nowadays, various KEP variances are used by internet protocol such as IKEv2/3. The purpose of KEP is to enable a secret key(s) sharing between two or more computing systems on unsecure network. Later, the secret key(s) is used to encrypt all data transmitted for online systems such as internet banking, cryptocurrency transaction, IoT services etc. The timing attack was addressed by an adversary model and security assumptions. The relay attack on KEP was tested by an experiment testbed between a key fob and car using Raspberry Pi and RF module. The experiment result has shown that the propagation delay of KEP on RF communication is increased by 100% for each relay node. If the KEP runtime is increased greater than 50%, the KEP authentication key should be discarded to prevent the attacker from gaining access to the car.

Corresponding Author:

Mohd Anuar Mat Isa,
Faculty of Electrical Engineering,
40450 UiTM Shah Alam, Selangor, Malaysia
Email: anuarls@hotmail.com

1. INTRODUCTION

After four decades since the first KEP introduced by Diffie-Hellman, many research works have been done to improve the original KEP based on the recently encountered security issues. This work explores the security of KEP against timing and relay attacks. The timing attack will provide additional information that can be used by an attacker in breaking a cryptographic communication protocol. This attack will reveal cryptographic runtimes during the secret key generation process, which could leak the secret key used in the KEP. For the relay attack, the attacker will relay RF frames through long distance and it can pretense as a legitimate node (device) while the legitimate node is far away. Most of the relay attack is applied for deceiving Radio-frequency Identification (RFID) access systems such as door and automotive entry. This work will address the most recently KEP by Isa M.A.M et al. [1], whereby the authors showed significant works on proving the security of KEP against various adversary models and side-channel security.

This paragraph will illustrate the paper organization as follows: This section provides an introduction to this work. Section 2 discuss the original DHKE and its cryptographic primitives. Section 3 will revisit the state of the art in KEP. Section 4 presents an adversary model for the timing attack. Section 5 presents an attack model for the relay attack. Section 6 will discuss the security analysis for the timing and relay attacks. Section 7 will show the experimental setup for the relay attack as well as the experiment results. Section 8 will discuss the results of the relay attack experiment and the timing attack security reduction. Section 9 discusses this paper contribution. Lastly, section 10 concludes the research work done by the authors and also offers an introduction to the future work.

2. DHKE BACKGROUND

Diffie-Hellman (1976) introduced the first key distribution protocol [2] which allows a secret to be shared in unsecure networks. Diffie-Hellman key exchange (DHKE) protocol had solved a traditional banking problem in sharing symmetric keys. Before DHKE, the symmetric keys were distributed by trusted human over the world. It required human and physical medium to share the symmetric keys between banks. At that moment, National Institute of Standards and Technology (NIST) Data Encryption Standard (DES) was used as a symmetric cryptosystem for banking. Through DHKE, the sharing symmetric keys problem in the traditional banking is solved. DHKE (1976) algorithm or DHKE textbook is presented as shown in Figure 1. DHKE relies on a discrete log problem as the foundation mathematical computation hardness, which is to find a root in modular arithmetic. The root is the private parameters a and b.

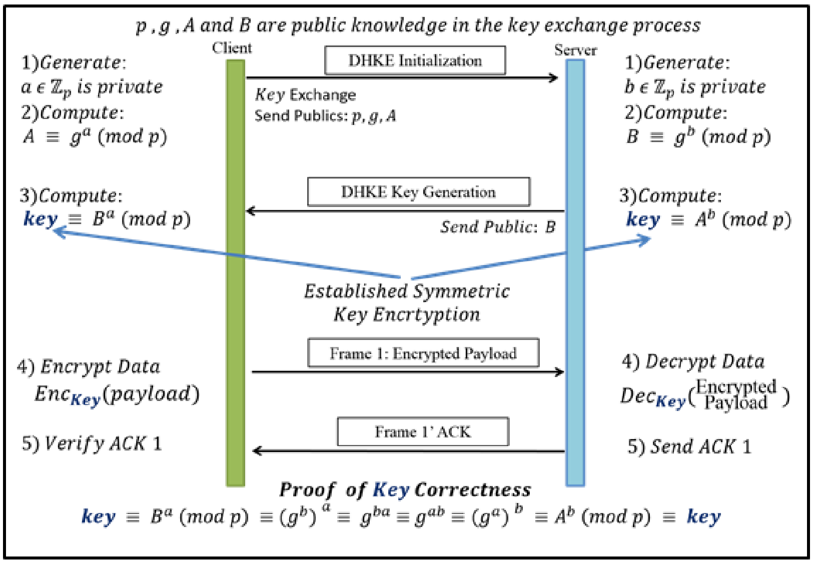


Figure 1. DHKE cryptosystem for exchange asymmetric key

3. RECENT WORKS ON KEY EXCHANGE PROTOCOL

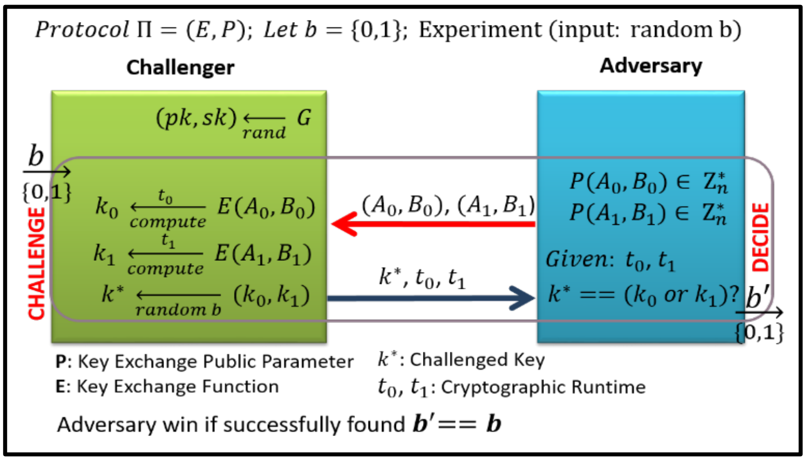
After four decades since its introduction, many research works have been done to improve DHKE based on recently encountered security issues. Arazi B. [3] (1993) proposed an integration of key exchange protocol and NIST digital signature standard (DSS) for establishing identity assurance for all key exchange protocol participants. Kocher P.C. [4] (1996) has shown a practical side-channel attack on KEP using timing attack for cryptographic computation. Raymond et al. (2002) [5] proposed a collective of attacks in the DHKE protocol and a good idea on how to securely implement the DH protocol in various systems. Harn L. et al. (2004) [6] proposed one, two and three rounds of DHKE and digital signature algorithm (DSA). R.C.W Phan (2005) [7] fixed problems in the fixed three-round DHKE DSA [6] by adding a forward secrecy and key freshness as required in a key exchange standard. Yoon et al. (2009) [8] proposed an efficient DHKE hash message authentication code (HMAC) with forward secrecy, key independence and protection against session state reveal attacks. The authors have claimed that their technique is more efficient than Jeong I.R. et al. [9]. Viet H.V. et al. (2013) [10] proposed two DHKE DSA protocols that have satisfied seven security attributes for a key exchange protocol to be assumed secure [10]–[12], namely known key authentication, forward secrecy, known-key security, unknown key-share attack, key relay attack, key freshness and session-state reveal [10] respectively.

Mandal S. et al. (2014) [13] propose a multi-party DHKE with perfect forward secrecy using a Trusted Third Party (TTP). The TTP functions as a group controller for all DHKE participants. Gola K.K. et al. (2015) [14] proposed a secure DHKE by implementing RSA encryption and decryption on DHKE secrets. Fathirad I. et al. (2016) [15] revisited DHKE commercial protocols for various network attacks such as man-in-the-middle, digital certificate (parameters on TLS/DTLS), signature on TLS/DTLS/IKEv2, signature on

SSH and TLS/DTLS, pre-shared key on TLS/DTLS, MAC on IPsec (IKEv2), EAP and third-party server on IKEv2, cached shared secret or SAS on ZRTP, DoS and reply respectively. Francillon et al. (2011) [16] from ETH Zurich have shown practical experiments that can be used to fool AKS through relay attacks using large timing delays for long distances and multiple relays for radio-hopping relays at long distances. The most recent work was done by Isa M.A.M. et al. (2017) [1] whereby a chain of KEP with relay attack detection is used to secure communication session between automotive (car) and keyfob (owner). The cryptosystem has been designed and proved by referring to the methods by Viet [10], Yoon [8], Jeong [28] and Harn [6]. The proposed KEP by Isa [1] can be used to secure symmetric encryption in networked systems [17]–[19].

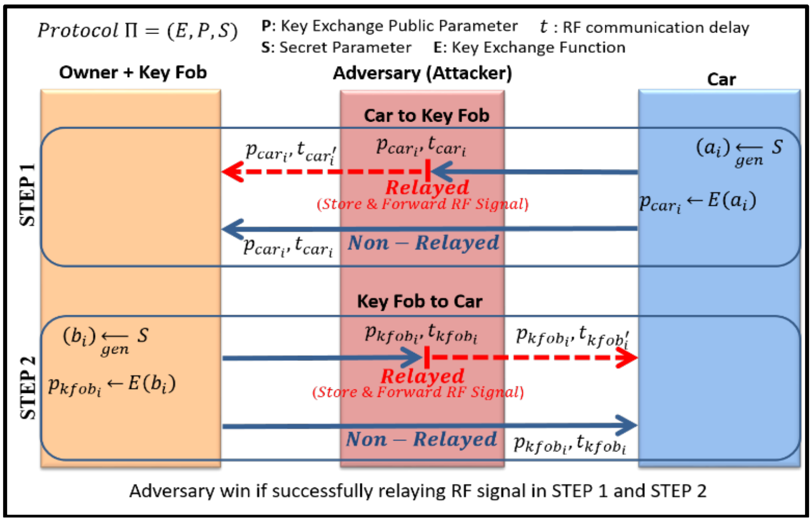
4. ADVERSARY MODEL FOR TIMING ATTACK

The paper has introduced an adversary model using an indistinguishability experiment with timing attacks on KEP. In this adversary model, an adversary has the knowledge of adaptive indistinguishability and timing knowledge that are accessible by an oracle. This model allows the adversary to access identical computing resources in terms of computing hardware (e.g. CPU). The adversary is given the knowledge of time t_i being the duration to perform cryptographic computations (e.g. primitive computation and protocol execution). Furthermore, the adversary has the knowledge of network transmission delay for all transactions as shown in Figures 2 and 3.



$Protocol\ \Pi = (E, P);\ Let\ b = \{0,1\};$ Experiment (input: random b)
Challenger
Adversary
$(pk, sk) \xleftarrow[rand]{} G$
b
$\{0,1\}$
CHALLENGE
$k_0 \xleftarrow[compute]{t_0} E(A_0, B_0)$
$k_1 \xleftarrow[compute]{t_1} E(A_1, B_1)$
$k^* \xleftarrow[random\ b]{} (k_0, k_1)$
$(A_0, B_0), (A_1, B_1)$
k^*, t_0, t_1
$P(A_0, B_0) \in Z_n^*$
$P(A_1, B_1) \in Z_n^*$
$Given:\ t_0, t_1$
$k^* == (k_0\ or\ k_1)?$
b'
$\{0,1\}$
DECIDE
P: Key Exchange Public Parameter
E: Key Exchange Function
k^*: Challenged Key
t_0, t_1: Cryptographic Runtime
Adversary win if successfully found $b' == b$

Figure 2. Indistinguishability experiment with timing attacks on KEP



$Protocol\ \Pi = (E, P, S)$
P: Key Exchange Public Parameter
t : RF communication delay
S: Secret Parameter
E: Key Exchange Function
Owner + Key Fob
Adversary (Attacker)
Car
STEP 1
Car to Key Fob
$p_{car_i}, t_{car_i'}$
p_{car_i}, t_{car_i}
$(a_i) \xleftarrow[gen]{} S$
$p_{car_i} \leftarrow E(a_i)$
Relayed
(Store & Forward RF Signal)
p_{car_i}, t_{car_i}
$Non-Relayed$
STEP 2
Key Fob to Car
$(b_i) \xleftarrow[gen]{} S$
$p_{kfob_i} \leftarrow E(b_i)$
p_{kfob_i}, t_{kfob_i}
$p_{kfob_i}, t_{kfob_i'}$
Relayed
(Store & Forward RF Signal)
$Non-Relayed$
p_{kfob_i}, t_{kfob_i}
Adversary win if successfully relaying RF signal in STEP 1 and STEP 2

Figure 3. A relay attack (one relay) between a key fob and car

For the indistinguishability experiment, the Adversary will send two pairs of public parameters $P(A_0, B_0)$ and $P(A_1, B_1)$ to the Challenger. Referring to Figure 2, the Challenger will compute key exchanges k_0 and k_1, and its cryptographic computational timings t_0 and t_1 for both public parameters $P(A_0, B_0)$ and $P(A_1, B_1)$. Then the Challenger will randomly choose either k_0 or k_1 as the challenged keyk^*. Altogether the k^*, t_0 and t_1 are sent to the Adversary. The Adversary needs to distinguish whether the key k^* is k_0 or k_1 with the additional information of timing t_0 and t_1. If the probability of guessing the correct key k^* is greater than $\frac{1}{2}$ as shown in Figure 3, then it can be concluded that the Adversary has the "advantage" and the given protocol $\prod$ is considered not secure in terms of indistinguishability experiment.

5. RELAY ATTACK

This section presents the relay attack by an experiment between a key fob and car. To mount the relay attack, an adversary will set up at least one radio frequency (RF) relay between the key fob and car, which will act as a man-in-the-middle during security authentication sessions between the key fob and car [16]. The relayed security authentication credentials will authorize the car to be locked or unlocked even though the car's owner (with the key fob) is far away from the car. By this attack, the adversary will succeed to fool the automotive keyless systems (AKS) using at least one or more RF relay nodes as shown in Figures 3 and 4. There is no an attempt to break cryptographic encryption key by the adversary, but through relaying the encrypted RF communication data between the key fob and car that makes the existing AKS vulnerable to the relay attack.

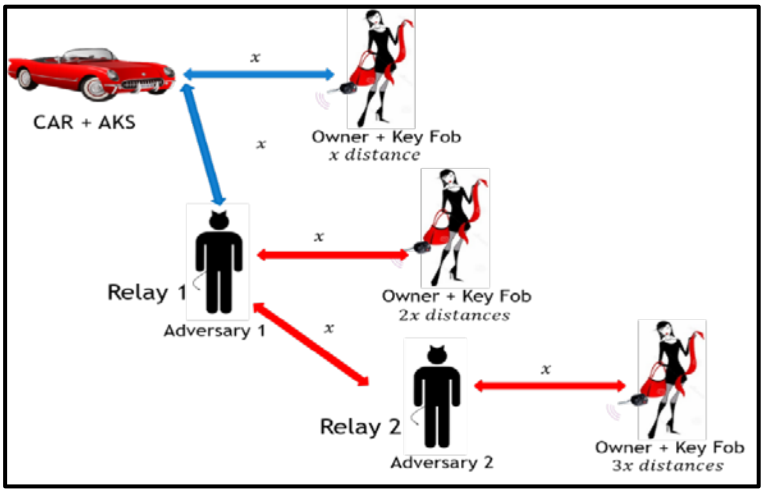


Figure 4. Adversaries relaying RF signal for long distance

This paragraph explains the relay attack between the key fob and car as shown in the Figure 3. In the Step 1, the car will send public parameter p_{car_i} for session i over RF. The p_{car_i} will arrive at the key fob either without a relay or relayed by the adversary. If without a relay, the p_{car_i} will be arrived at the key fob by a transmission delay t_{car_i} for x distance. If relayed by the adversary, the p_{car_i} will be arrived at the adversary by a transmission delay t_{car_i} for x distance. Then the adversary will forward the p_{car_i} to the key fob by a transmission delay $t_{car_i'}$ for x distance. Therefore the total transmission delay by the adversary is $t_{car_i} + t_{car_i'}$ for $2x$ distances. In this case, the car owner (hold key fob) is assumed that he/she is unable to see the car at $2x$ distances. This will grant an opportunity to the adversary to mount the relay attack between the car and key fob at the $2x$ distances.

In the Step 2, the key fob will send public parameter p_{kfob_i} for session i over RF. The p_{kfob_i} will arrive at the car either without relay or relayed by the adversary. If without a relay, the p_{kfob_i} will be arrived at the car by a transmission delay t_{kfob_i} for x distance. If relayed by the adversary, the p_{kfob_i} will be arrived at the adversary by a transmission delay t_{kfob_i} for x distance. Then the adversary will forward the p_{kfob_i} to the car by a transmission delay $t_{kfob_i'}$ for x distance. Therefore the total transmission delay by the adversary is

$t_{kfob_i} + t_{kfob'_i}$ for $2x$ distances. The following equations show the examples of RF communication delay without relay attack and with relay attack:
Without relay attack:

$$delay_i = t_{car_i} + t_{car'_i}$$

With one relay attack:

$$delay'_i = t_{car_i} + t_{car'_i} + t_{kfob_i} + t_{kfob'_i}$$

6. SECURITY ANALYSIS

This section presents the security analysis for timing and relay attacks as follows:

6.1. Timing Attack

Adversary model: Indistinguishability experiment for key exchange protocol.

Adversary knowledge: $\mathrm{P(A_0, B_0)}$, $\mathrm{P(A_1, B_1)}$, $\mathrm{P(A_i, B_i), t_0, t_1, t_i}$ and $\mathrm{k_i}$.

Adversary limitation: The adversary cannot access the challenged keys $\mathrm{k_0}$ and $\mathrm{k_1}$ from $\mathrm{P(A_0, B_0)}$ and $\mathrm{P(A_1, B_1)}$ by the oracle for a fair indistinguishability experiment.

Oracle key exchange computation: The oracle knows all secret parameters (e.g. $\mathrm{a_i, b_i}$) that are required to compute $\mathrm{k_0, k_1, k_i}$ by public parameters $\mathrm{P(A_0, B_0), P(A_1, B_1), P(A_i, B_i)}$. The oracle also shares the timings $\mathrm{t_0, t_1, t_i}$ as requested by the Adversary that gives additional knowledge to mount the timing attacks.

Security assumptions: 1) Computational Diffie-Hellman (CDH) problem is hard in the cyclic group G; 2) hash function is a hash function with strong collision-resistant [20]; and 3) a fixed-time of KEP runtime for all fixed input length into the key exchange function that runs in a polynomial time, whereby the key exchange function receives any valid input with the same length (e.g., f(101) and f(001), where |f(101)|=|f(001)|) will have the identical runtime or execution for all conditions. The fixed-time is based on the worst-case scenario to compute the KEP runtime.

Security reductions: The problem of finding a key $\mathrm{k^*}$ is reduced to the problem of indistinguishability experiments for large n experiment sessions. The $\mathrm{k^*}$ satisfies the indistinguishability experiments for key exchange protocol if and only if the adversary advantage $\mathrm{\varepsilon(n)}$ is negligible for the large n experiment sessions.

Security arguments: By the security assumptions 1), 2) and 3), the advantage over probabilistic polynomial-time (PPT) negligible. If the worst case fixed-time cryptographic computation is implemented in KEP, the Adversary will not be able to distinguish whether the key k^* is $k_0 \; or \; k_1$ with the additional information of timing t_0 and t_1. The worst case fixed-time cryptographic computations will render the Adversary capability to mount the timing attacks on the KEP implementation almost infeasible because timing t_0 and t_1 are not the actual KEP cryptographic runtimes. Therefore, the Adversary lost in the indistinguishability experiment by the negligible advantage.

6.2 Relay Attack

Attack model: Relay Attack on KEP

Adversary knowledge: $\mathrm{p_{car_i}}$ and $\mathrm{p_{kfob_i}}$

Relay attack experiment: The Adversary will relay all encrypted RF communication data between the key fob and car as shown in Figure 3.

Adversary limitation: The Adversary may deploy more than one RF relay nodes for an extensive distance between the key fob and car, but it will introduce more RF transmission delays. This assumption is also included that the adversary cannot access or directly temper the key fob and car.

Adversary goal: To lock or unlock the car (or driveway the car) using the relay attack.

Adversary computation: The Adversary will implement store and forward of all encrypted RF communication data between the key fob and car in one or more RF relay nodes as shown in the Figures 3 and 4.

Security assumptions: It is identical to the security assumptions 1 until 3 in the timing attack. In addition to the timing attack security assumptions, 4) any relayed RF communication data between the key fob and car will introduce RF transmission delays $\mathrm{t_{car'_i}}$ and $\mathrm{t_{kfob'_i}}$ because of the implementation of store and forward by one or more RF relay nodes. 5) If KEP implements RF communication delay detection (or RF timeout) between the key fob and car, it can detect the RF transmission delays $t_{car'_i}$ and $t_{kfob'_i}$ that are introduced by the relay attack node(s) because of the worst-case scenario of the KEP in RF communication delays are t_{car_i} and t_{kfob_i}.

Security reduction: The problem of relaying KEP for RF communication data is reduced to the problem of not introducing RF transmission delays $t_{car_i'}$ and $t_{kfob_i'}$ between the key fob and car for x distance. The KEP satisfies the security against relay attack if and only if the Adversary is not able to lock or unlock the car (or driveway the car) using the relay attack by $2x$ distance. One may refer to RF communication between the key fob and car for the relay attack experiments using chained KEP (CKEP) proposed by M.A.M Isa et al. [1], [21], [22] in the next section. There are three experimental setups for the x distance, namely 1, 2.5 and 5 meters.

7. RELAY ATTACK EXPERIMENT

7.1 Experiment Setup

Figure 4 shows the experiment setup for CKEP public parameter exchanges over RF without a relay, one relay node and two relay nodes respectively. This work has selected CKEP that proposed by M.A.M Isa et al. [1], [21], [22] as KEP for the relay attack experiment. The experiment setup was used to measure time of flight (ToF) of RF communication by a round trip time (RTT) distance estimation method [23], [24]. Table 1 shows hardware and software used for the relay attack experiment.

Table 1. Hardware and software for relay attack experiment

Testbed Setup	Descriptions
Hardware	Raspberry Pi 2 Model B, 900MHz ARM Cortex-A7 CPU (overclock to 1 GHz), Quad Cores CPU, L1 32 KB (each core) and L2 512 KB (shared) caches and 1GB RAM. Ciseco Slice of Radio: SRF Radio Module with on-board "chip" antenna (Texas Instruments CC1110-CC1111).
Software	Raspbian 8 (Jessie) OS, Linux Kernel 4.4.21-v7+ and Python 3.42.

7.2 Experiment Results

The results in Figure 5 has shown that the average propagation delay for 1, 2.5 and 5 meters that are consistent (value very close) by the given simulation distances due to “the propagation speed of radio waves in air approaches the speed of light” [23]. For example, the propagation delay of CKEP (without relay) for 1 meter is 0.008663, 2.5 meter is 0.008542 and 5 meter is 0.008588 respectively. The results have shown that the propagation delay on RF for one relay is increased by 101.1% and for two relays is increased by 210.4%. The propagation delay on RF allows one to detect a relay attack(s) is being mounted by one or more relay nodes. Referring to the equation (1), one may use the given equation to detect the relay attack between a car and key fob whereby an authentication key must be discarded due to RRF $>$ WRF. The authentication key (cryptographic key) is used to lock/unlock or start car engine if the CKEP successfully verified. In general, the propagation delay on RF is increased by 100% for each relay node, e.g. if three relays are presented, then the RF propagation delay could be increased by at least 300%.

Based on the experiment results of the relay attack as shown in the Figure 5, if an adversary mounts the relay attack, then it will introduce the RF communication delay as the following Equation:

$$\text{RRF} > \text{WRF} \tag{1}$$

Whereby:

RRF is the total time of RF communication (including relayed RF).

WRF is the time of the worst-case CKEP RF communication delay (expected delay).

If ($\text{RRF} > W\mathit{RF}$), then the CKEP authentication key will be discarded and the car is safe from the relay attack.

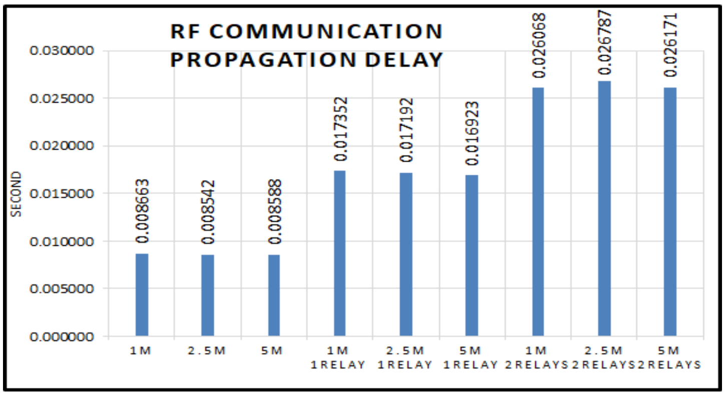


Figure 5. The comparison of CCAP communication propagation delay over RF

8. DISCUSSION

This work has conducted experiments for evaluating the security of KEP against timing and relay attacks. Referring to the security analysis for timing attack in Section 4, the fixed-time of KEP runtime (security assumption 3) can be deployed to prevent an attacker(s) from gaining an advantage to break KEP using timing attack. Another method to prevent the timing attack using blinding in KEP cryptographic computation [4], [25]. However, this method will increase cryptographic computation runtime compared to the fixed KEP runtime. Blinding will create different KEP runtime for the same input parameters, which will give misleading timing information to the attacker in mounting the timing attack. Furthermore, to secure KEP from the relay attack as aforementioned in Sections 6 and 7, the runtime for KEP must be closest to the fixed runtime because it will help CKEP to detect RF communication delay when the attacker(s) is deploying RF relay node(s) between car and keyfob. If the runtime KEP is not fixed, it is difficult to compare the runtime of without relay and relayed RF communication. Referring to the experiment results for relay attack using CKEP, when the CKEP runtime is increased by 50%, the CKEP authentication key should be discarded to prevent the attacker from gaining access to the car. The experiment results have also shown that the propagation delay on RF communication is increased by 100% for each relay node. This will help in detecting the number of relay nodes that are being used during the relay attack between car and keyfob.

9. CONTRIBUTION

This paper has improved KEP security by suggesting a method to detect and prevent both timing and relay attacks. The fixed-time of KEP runtime can help to prevent the timing attack with a low computing cost compared to the blinding method. Furthermore, the fixed-time of KEP runtime (e.g. CKEP) can be used to detect and secure an automotive system from the relay attack. This method will enable the CKEP to calculate the RF propagation delay which either there is RF relay node(s) between car and keyfob, or direct RF communication between car and keyfob. This will prevent the relay attack that was successfully tested by ETH Zurich research lab [16].

10. CONCLUSION

This paper has revisited the state of art of KEP which presented in Sections 2 and 3. Based on the review, this work found none of the precedent work has tested the KEP security against the relay attack by experimental testbed. This work has presented the method to detect and prevent both timing and relay attacks in KEP. The fixed-time of KEP runtime can be used to detect both attacks. For the future work, the authors will explore other side-channel attacks on KEP such as power analysis attack.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the Ministry of Education (MOE) Malaysia for providing the grant 600-RMI/NRGS 5/3 (5/2013), and Universiti Teknologi MARA (UiTM) for supporting this research work.

REFERENCES

[1] Mohd Anuar Mat Isa, Hashim, H., Adnan, S. F. S., Marbukhari, N. and Mohamed, N. N., "An automobile security protocol: Side-channel security against timing and relay attacks", *International Journal of Electronic Security and Digital Forensics*, vol. 9, no. 3, pp. 239–253, 2017.

[2] Diffie, W. and Hellman, M. E., "New Directions in Cryptography", in *IEEE Transactions on Information Theory*, 1976, pp. 644–654.

[3] Arazi, B., "Integrating a key distribution procedure into the digital signature standard", in *Electronics Letters*, 1993, vol. 29, no. 11, p. 966.

[4] Kocher, P., "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", in *Advances in Cryptology—CRYPTO'96*, 1996.

[5] Raymond, J. and Stiglic, A., "Security issues in the Diffie-Hellman key agreement protocol", in *McGill University Technical Manuscript*, 2002.

[6] Harn, L., Mehta, M. and Hsin, W.-J., "Integrating Diffie-Hellman Key Exchange into the Digital Signature Algorithm (DSA)", *IEEE Communications Letters*, vol. 8, no. 3, pp. 198–200, 2004.

[7] Phan, R. C., "Fixing the Integrated Diffie-Hellman-DSA Key Exchange Protocol", *IEEE Communications Letters*, vol. 9, no. 6, pp. 570–572, 2005.

[8] Yoon, E. J. and Yoo, K. Y., *"An efficient Diffie-Hellman-MAC key exchange scheme"*, in 2009 4th International Conference on Innovative Computing, Information and Control, ICICIC 2009, 2009, pp. 398–400.

[9] Jeong, I. R., Kwon, J. O. and Lee, D. H., "Strong Diffie-Hellman-DSA key exchange", *IEEE Communications Letters*, vol. 11, no. 5, pp. 432–433, 2007.

[10] Viet, H. Van, Minh, N. H., Truyen, B. T. and Nga, N. T., *"Improving on the Integrated Diffie-Hellman-GOST . R94 Key Agreement Protocols"*, in Third World Congress on Information and Communication Technologies (WICT), 2013, pp. 105–109.

[11] Canetti, R. and Krawczyk, H., "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels", in *Advances in Cryptology — EUROCRYPT 2001*, 2001, pp. 453–474.

[12] Menezes, A. J., Oorschot, P. C. Van and Vanstone, S. A., *Handbook of Applied Cryptography*, 5th ed. CRC Press, 1996.

[13] Mandal, S. and Mohanty, S., *"Multi-party key-exchange with perfect forward secrecy"*, in 2014 13th International Conference on Information Technology, ICIT 2014, 2015, no. May, pp. 362–367.

[14] Gola, K. K., Rathore, R., Sharma, V. and Kandpal, M., *"Secure Key Exchange in Diffie Hellman Key Exchange Algorithm"*, in International Conference of Advance Research and Innovation (ICARI-2015), 2015, pp. 473–475.

[15] Fathirad, I., Devlin, J. and Atshani, S., "Network-Specific Attacks on Diffie-Hellman Key-Exchange in Commercial Protocols", *International Journal of Computer Theory and Engineering*, vol. 8, no. 2, p. 129, 2016.

[16] Francillon, A., Danev, B. and Capkun, S., "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars", *Network and Distributed System Security Symposium*, pp. 431–439, 2011.

[17] Arivazhagan, A., "RTL Modelling for the Cipher Block Chaining Mode (CBC) for Data Security", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 3, pp. 709–711, 2017.

[18] Choi, Y., "Cryptanalysis on Privacy-Aware Two-Factor Authentication Protocol for Wireless Sensor Networks", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 2, pp. 296–301, 2017.

[19] Awadalla, M., Al Maashri, A., Pathuri, L. and Ahmad, A., "Customized hardware crypto engine for wireless sensor networks", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 7, no. 1, pp. 263–275, 2017.

[20] Cramer, R. and Shoup, V., "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack", in *Lecture Notes in Computer Science: Advances in Cryptology—CRYPTO'98*, 1998, pp. 1–18.

[21] Mohd Anuar Mat Isa, Hashim, H., Manan, J. A., Adnan, S. F. S. and Mahmod, R., "A Series of Secret Keys in a Key Distribution Protocol", in *Transactions on Engineering Technologies: World Congress on Engineering and Computer Science 2014*, 2015, pp. 193–207.

[22] Mohd Anuar Mat Isa, Habibah Hashim, Jamalul-lail Ab Manan, Syed Farid Syed Adnan and Ramlan Mahmod, "An Experimental Study of Cryptography Capability using Chained Key Exchange Scheme for Embedded Devices", in *Lecture Notes in Engineering and Computer Science*, 2014, vol. 1, pp. 510–515.

[23] Markantonakis, K. and Mayes, K., *Secure smart embedded devices, platforms and applications*. Springer-Verlag New York, 2014.

[24] Goel, U., Wittie, M. P., Claffy, K. C. and Le, A., "Survey of end-to-end mobile network measurement testbeds, tools, and services", *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1. pp. 105–123, 2016.

[25] Garrett, D. and Ward, M., *"Blinded Diffie-Hellman: Preventing Eavesdroppers from Tracking Payments"*, in International Conference on Research in Security Standardisation, 2014, pp. 79–92.