Journal of Computer Science
https://dergipark.org.tr/en/pub/bbd
https://doi.org/10.53070/bbd.990849

Journal of Computer Science
ISSN: 2548-1304
Volume: IDAP-2021, Issue: Special, pp: 385-390
@Anatolian Science

Nesnelerin İnternetinde Çok Katmanlı Algılayıcı Kullanarak Zamanlama Analizi Saldırısı ile Özel Anahtar Tahminlemesi

Timing Analysis Attack For Private Key Prediction Using Multilayer Perceptron in IoT

Muhammed Saadetdin KAYA [*1], Kenan İNCE [2]

[1]Bilgisayar Mühendisliği Bölümü, İnönü Üniversitesi, Malatya, TÜRKİYE

[2]Bilgisayar Mühendisliği Bölümü, İnönü Üniversitesi, Malatya, TÜRKİYE

(saadetdin.kaya@gmail.com, kenanince@gmail.com)

Received: Sep.3, 2021 Accepted: Sep.16,2021 Published: Oct.20, 2021

Özetçe— Doğrudan kaynağa erişim olmasa bile, gizlenmek istenen veriler hakkında bilgi sahibi olunmasını sağlayan yan kanal saldırılarından biri olan Zamanlama Analizi Saldırıları; bir işlemin veya algoritmanın farklı şartlar altında harcadığı sürelerin yorumlanmasıyla, sistem hakkında bilgi edinmeyi amaçlayan bir saldırı türüdür. Bu çalışmada, belirlenmiş bir senaryodaki özel anahtarın zamanlama analizi yöntemiyle Çok Katmanlı Algılayıcı (MLP – Multilayer Perceptron) kullanılarak sistem analiz edilmiştir. Analiz sonucunda zamanlama bilgisi kullanılarak gizli anahtarın tahminlenmesi amaçlanmıştır. Yapılan çalışma sonucunda sunulan yöntemle, %95'in üzerinde doğruluk oranına sahip bir şekilde gizli anahtar tahminlenmiş olup, Nesnelerin İnterneti (IoT – Internet of Things) alanında zamanlama analizi saldırılarının ciddi bir tehdit oluşturabileceği ortaya koyulmuştur.

Anahtar Kelimeler : *Yan-kanal Saldırıları, Zamanlama Analizi Saldırıları, Çok Katmanlı Algılayıcı, Nesnelerin İnterneti*

Abstract— Timing Analysis Attacks are one of the side channel attacks that allows to be informed about the data that is wanted to be hidden, even if there is no direct access to the source. It is a type of attack aimed at learning about the system by interpreting the amount of time that a process of algorithm spends under different circumstances. In this study, the system was analyzed using a multilayer sensor (MLP – Multilayer Perceptron) by timing analysis of the private key in a specified scenario. As a result of the analysis, it is aimed to estimate the secret key using timing information. As a result of the analysis, it is aimed to estimate the secret key using timing information. As a result of the study, the secret key was estimated with an accuracy rate of more than 95% and it was revealed that timing analysis attacks could pose a serious threat in the Internet of Things (IoT) area.

Keywords : *Side-channel Attacks, Timing Analysis Attacks, Multilayer Perceptron (MLP), Internet of Things (IoT)*

1.Giriş

Bir işlemin ne kadar sürede yapıldığı, yapılırken harcanan güç, ortaya çıkan elektromanyetik yayınım, işlem süresince çıkan sesin şiddeti gibi sistem dışına istemsiz çıkışlar gerçekleşmektedir. Bu

istemsiz çıkışlar sistemin çözümlenmesinde kullanılabilecek nitelikte ise bu bilgiler yan-kanal bilgisi olarak adlandırılırlar. Yan-kanal analizi saldırıları (YAS) bu istemsiz çıkışlar vasıtasıyla sistem hakkında bilgi edinmeyi veya çözümlenme sağlanmasını hedeflemektedirler. Lakin aynı işlem, farklı uygulamalarında değişik bilgiler ortaya çıkarabilir, bu nedenle YAS'lar her sistem için o sistemin özelinde gerçekleştirilmelidir.

Yan-kanal analizi saldırıları, genel olarak aktif saldırılar ve pasif saldırılar olmak üzere iki grupta incelenmektedirler. Aktif saldırılar ya da diğer adıyla kurcalama saldırıları (Anderson ve Kuhn, 1996) kriptografik cihazın içindeki devrelere ulaşmasını gerektirirler (Ordu ve Yalçın, 2016). Pasif saldırılar, sistemin çalışmasına doğrudan müdahale etmeden üretmiş olduğu yan–kanal bilgilerinden faydalanırlar.

1996 yılında Kocher yaptığı çalışma ile pasif saldırıların önemini ortaya koymuştur (Kocher, 1996). Pasif saldırılar analiz sırasında kullanılan yönteme göre isimlendirilirler. Yaygın olarak kullanılan pasif yan-kanal saldırıları; Güç Analizi Saldırıları, Elektromanyetik Analizi Saldırıları ve Zamanlama Analizi Saldırılarıdır.

Donanıma doğrudan erişime ihtiyaç duymadan uygulanabilen ve gerçekleştirilmesi görece daha kolay olan Zamanlama Analizi Saldırıları (ZAS) bir işlemin veya algoritmanın çeşitli şartlar altında değişen işleme süresinin yorumlanmasıyla sistem hakkında bilgi edinmek amacıyla yapılan bir saldırı türüdür. Bu saldırı türünde saldıran şartları değiştirerek çok sayıda saldırı düzenler ve değişen şartlar ile işleme süresi arasında anlaşılabilir bir ilişki kurmayı hedefler.

İnsanlar tarafından kurulamayan veya çok zor kurulan ilişkilerin bilgisayarlar tarafından makine öğrenmesi ile kolaylıkla kurulabildiği görülmüştür (Libbrecht ve Noble, 2015; Korou vd., 2015; Vovk vd., 1999). Çok Katmanlı Algılayıcılar sayesinde büyük sayıdaki veriler yorumlanarak o verilerin kaynağı olan sistemler hakkında çeşitli modeller ortaya konulmaktadır (Gardner ve Dorling, 1998; Isa ve Mamat, 2011; Hontoria vd., 2005). Zamanlama Analizi gibi doğru analiz yapılabilmesi için yorumlama hassasiyetinin yüksek, yorumlanması gereken veri sayısının çok olduğu analiz yöntemlerinde Çok Katmanlı Algılayıcılar'ın kullanımı siber güvenlik alanında son dönemde oldukça yaygınlaşmıştır (Teoh vd., 2018; Ben Fredj vd., 2020)

Nesnelerin İnterneti (IoT – Internet of Things) konseptinin yaygınlaşması ile birlikte IoT cihazlarının saldırı tespiti noktasındaki yetersizliği gün geçtikçe daha da belirginleşmektedir (Liu vd., 2011; Ullah vd., 2019; Zarpelão vd., 2017). Bununla birlikte makine öğrenmesi kullanılarak yapılan saldırılar ve bu saldırıların çeşitlilikleri de aynı oranda artmaktadır (Aseeri vd., 2018; Anitha ve Arockiam, 2019).

Bu çalışmada, Zamanlama Analizi Saldırısı (ZAS), bir IoT ekosisteminde özel anahtar eşleştirme senaryosun kullanılarak simüle edilmiş olup Çok Katmanlı Algılayıcı aracılığıyla; işleme süresi ile girdi ve özel anahtar arasındaki benzerliğe bakılarak etiketleme işlemi yapılmıştır. Bu sayede model optimize edilmiş olup ileride yapılabilecek herhangi bir girdinin, süresine göre özel anahtar ile benzerliğinin tahmin edilip edilemeyeceği test edilmiştir.

2. VERİ SETİNİN OLUŞTURULMASI

Tahminleme işleminin doğru sonuçlar verebilmesi için kullanılacak veri setinin kapsayıcı olması, yeterli sayıda örnek barındırması, nominal bir dağılıma sahip olması ve yine sistem ihtiyacını karşılayacak bilgileri içinde barındırması gerekmektedir.

Uygun bir veri seti oluşturmak amacıyla çalışmada kullanılan veriler; özel anahtarla değişken benzerlik oranlarına sahip, rastgele oluşturulan girdilerin farklı şartlar altında her bir benzerlik grubu için 50.000 kez kullanılarak çalıştırılmasıyla oluşturulmuştur. Girdi, girdi-özel anahtar benzerliği ve işlem süresi kayıt altına alınmıştır.

3. ZAMANLAMA ANALİZİ SALDIRISI

Zamanlama Analizi Saldırılarında (ZAS) sabit veri işleme zamanına sahip olmayan algoritmaların sızdırdığı zamanlama yan-kanal bilgisinden faydalanılır. Bu durum, algoritma doğrudan çözülmese dahi saklanması istenilen veriye erişimi kolaylaştırır. Kocher (1996), Janke ve Laackmann (2002) daha önceki çalışmalarında işlemlerin yürütülme sürelerindeki farklardan faydalanarak elde edilen zamanlama yan-kanal bilgisi ile gizli bilgiye ulaşmayı başarmışlardır

Çalışmada, ZAS, girdinin mevcut veri ile eşleşme oranına göre; işleme süresinin yorumlanması yoluyla gizlenmek istenen verinin tahmin edilebilmesi amacıyla kullanılmıştır.

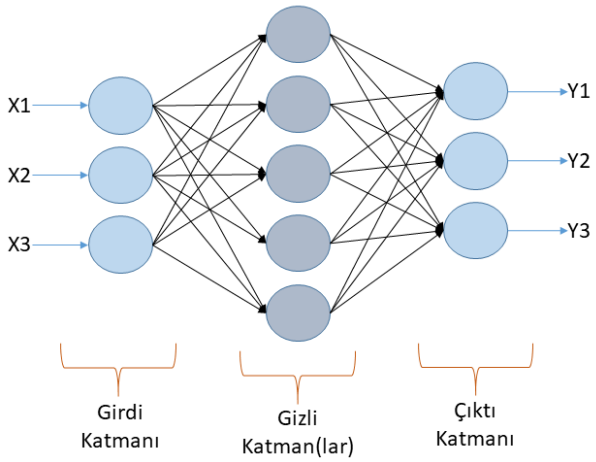
4. ÇOK KATMANLI ALGILAYICILAR

Yapay sinir ağları, canlılarda bulunan sinir sisteminden esinlenilerek ortaya çıkmış makine öğrenmesi alanında karmaşık sistemleri modellemek ve çözmek için kullanılan yapılardır. İnsan beynine benzer bir şekilde modellenmiş olan bu yapılar bilgisayarlara öğrenme yeteneği kazandırma amacıyla kullanılmaktadırlar (Öztemel, 2003). Diğer makine öğrenmesi yaklaşımlarından farklı olarak bu yapılarda öğrenme doğrudan örnekler aracılığı ile gerçekleşmektedir. Bu durum, öğrenme aşamasının uzun ve yorucu olmasına karşılık olarak doğru şekilde kullanılması halinde test aşamasının minimum hata ile oldukça hızlı şekilde gerçekleşmesine olanak sağlamaktadır.

Yapay sinir ağlarında bulunan 3 farklı öğrenme yönteminden biri olan öğretmenli öğrenme, çok katmanlı algılayıcıların temelini oluşturan öğrenme yöntemidir (Öztemel, 2003). Bu yöntem sayesinde, yönetilebilir bir metot olan, ileri beslemeli – geri yayılımlı algoritma Çok Katmanlı Algılayıcılar'da kullanılabilmektedir. Bu sayede, soru ile birlikte cevabın da girdi olarak öğrenme aşamasına dahil edilmesi ve etiketleme işleminin probleme uygun olarak yapılması sağlanmaktadır.

Şekil 1.'de görüldüğü üzere Çok Katmanlı Algılayıcılar 3 farklı grupta nitelendirilen katmanlardan oluşmaktadır. Bu katmanlar, gelen bilgilerin öğrenme işleminin gerçekleştirilmesi amacıyla alındığı ve gizli katmana yönlendirildiği girdi katmanı, bir veya birden fazla sayıda olabilecek, öğrenme işleminin gerçekleştirildiği gizli katman ve bilgi çıkışının sağlandığı çıkış katmanı olarak adlandırılmaktadır.

Bu çalışmada, girdi sayısının çokluğu ve verilerin birbirlerine benzerlikleri sebebiyle 5 adet gizli katman kullanılmıştır.



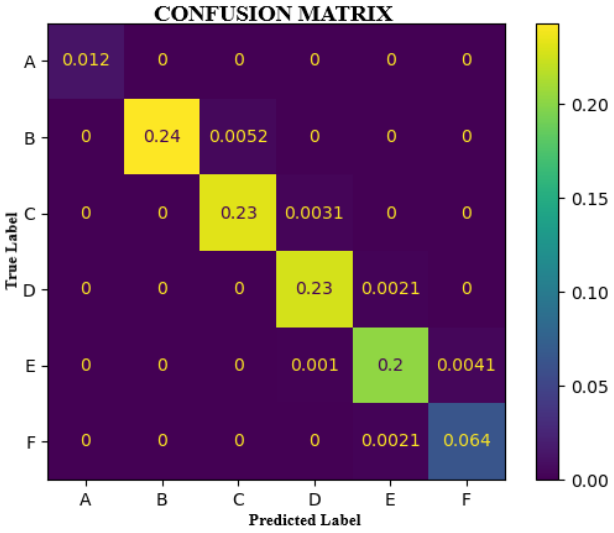
Şekil 1. Üç Girdili Bir Gizli Katmanlı ve Üç Çıktılı Bir Çok Katmanlı Algılayıcının Topolojik Yapısı

Çalışmada, oluşturulan veri seti, eğitim ve test verileri olarak iki gruba ayrılmıştır. Eğitim amacıyla ayrılan veri seti başlangıçta ağırlık vektörü rastgele olarak, öğrenme oranı ve azami iterasyon sayısı çeşitli denemeler sonucunda belirlenmiş olup Çok Katmanlı Algılayıcıya girdi olarak verilmiştir. Eğitim amacı; işleme süresine yardımıyla girdi-gizli anahtar benzerlik oranının etiketlenmesi olarak

belirlenmiştir. Eğitim işleminin her iterasyonunda ileri yayılım işlemi uygulanmış olup gerçek değer-tahmin farkının kritik değerin üzerinde olduğu durumlarda geri yayılım işlemi ağ üzerinde geriye dönük olarak dereceli azalma sağlanmış ve yeni ağırlık vektörü hesaplanarak iterasyona devam edilmiştir. Tahmin sonuçları istenen düzeye ulaştığında etiketleme yapılmış ve sonuçlar analiz edilmiştir.

5. SONUÇLAR VE TARTIŞMA

Oluşturulan veri seti kullanılarak yapılan eğitim sonucu elde edilen model kullanılarak yapılan etiketleme işlemi ile ortaya çıkan karmaşıklık matrisi Şekil 2.'de gibi görülmektedir.



Şekil 2. Test Sonuçları ile Oluşturulan Karışıklık Matrisi

Eğitim sonucunda oluşturulan model 10.000 farklı işleme süresi ile test edilmiş olup işleme süresine göre ait girdi ile gizli anahtar benzerliği gruplandırılmıştır. Bu gruplandırma Şekil 2.'deki gibi olup model, %98.24 doğruluk yüzdesiyle tahminleme işlemini gerçekleştirmiştir. Bu oran, dışarıya her türlü bilgi çıkışının engellenmesinin önemli olduğu siber güvenlik ve kriptografi alanları için çok yüksektir. Tasarlanan yöntem, yalnızca bu çalışmada uygulanan algoritmada değil, girdiye bağlı olarak değişen tepki süresine sahip herhangi bir algoritmada veya sistemde uygulanabilecektir Şekil 2.'de görülen sınıflar (A,B,C,D,E,F) Tablo 1.'deki yüzdelik bölümlere karşılık gelmektedirler.

Tablo 1. Karışıklık Matrisindeki Sınıflar ve Benzerlik Oranı İlişkisi

Sınıf	Benzerlik oranı (K)
A	$0 \leq K < 1$
B	$1 \leq K < 25$
C	$25 \leq K < 50$
D	$50 \leq K < 75$
E	$75 \leq K < 99$
F	$99 \leq K \leq 100$

İşleme süresinin sistemin anlık yükünün, kullanılan kaynaklar vb. değişkenler sebebiyle doğrudan yorumlanabilir olmamasına karşın Çok Katmanlı Algılayıcılar kullanılarak yorumlanabileceğini ortaya koyulmuştur. Bu nedenle algoritma tasarımı esnasında işleme süresinin girdiye bağlı olmayacak şekilde

tasarlanması veya tasarlanan algoritmanın sabit işleme süresine sahip olacak şekilde kurgulanması gibi önlemler alınması gerekmektedir.

Algoritma tasarımı esnasında alınacak önlemlerin fazla kaynak tüketimine yol açmaması ve sistemi yavaşlatmaması, düşük donanımsal özelliklere sahip olan ve genellikle hızlı tepki süresinin önem arz ettiği IoT sistemlerine uygun bir şekilde uygulanması gerektiği unutulmamalıdır.

Teşekkür

Bu çalışma, İnönü Üniversitesi Bilimsel Araştırma Projeleri Bölümü'nün (BAPB) FBG-2020-2143 sayılı projesi ile desteklenmiştir. Yazar, değerli geri bildirimleri için İnönü Üniversitesi BAPB'ye teşekkür eder.

Kaynaklar

Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Annual International Cryptology Conference (pp. 104-113). Springer, Berlin, Heidelberg.

Janke, M., & Laackmann, P. (2002). Power and timing analysis attacks against security controllers. Infineon Technologies AG, Technology Update, Smart Cards.

Anderson, R., & Kuhn, M. (1996, November). Tamper resistance-a cautionary note. In Proceedings of the second Usenix workshop on electronic commerce (Vol. 2, pp. 1-11).

Ordu, L., & Yalçın, S. B. Ö. (2016, December) Yan-Kanal Analizi Saldırılarına Genel Bakış.

Öztemel, E. (2003). Yapay sinir ağlari. PapatyaYayincilik, Istanbul.

Libbrecht, M. W., & Noble, W. S. (2015). Machine learning applications in genetics and genomics. Nature Reviews Genetics, 16(6), 321-332.

Kourou, K., Exarchos, T. P., Exarchos, K. P., Karamouzis, M. V., & Fotiadis, D. I. (2015). Machine learning applications in cancer prognosis and prediction. Computational and structural biotechnology journal, 13, 8-17.

Vovk, V., Gammerman, A., & Saunders, C. (1999). Machine-learning applications of algorithmic randomness.

Gardner, M. W., & Dorling, S. R. (1998). Artificial neural networks (the multilayer perceptron)—a review of applications in the atmospheric sciences. Atmospheric environment, 32(14-15), 2627-2636.

Isa, N. A. M., & Mamat, W. M. F. W. (2011). Clustered-hybrid multilayer perceptron network for pattern recognition application. Applied Soft Computing, 11(1), 1457-1466.

Hontoria, L., Aguilera, J., & Zufiria, P. (2005). An application of the multilayer perceptron: solar radiation maps in Spain. Solar energy, 79(5), 523-530.

Teoh, T. T., Chiew, G., Franco, E. J., Ng, P. C., Benjamin, M. P., & Goh, Y. J. (2018, July). Anomaly detection in cyber security attacks on networks using MLP deep learning. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-5). IEEE.

Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., & Derhab, A. (2020, November). CyberSecurity attack prediction: a deep learning approach. In 13th International Conference on Security of Information and Networks (pp. 1-6).

Aseeri, A. O., Zhuang, Y., & Alkatheiri, M. S. (2018, July). A machine learning-based security vulnerability study on xor pufs for resource-constraint internet of things. In 2018 IEEE International Congress on Internet of Things (ICIOT) (pp. 49-56). IEEE.

Anitha, A. A., & Arockiam, L. (2019). ANNIDS: artificial neural network based intrusion detection system for Internet of Things. Int. J. Innov. Technol. Explor. Eng. Regul, (2019), 8.

Liu, C., Yang, J., Chen, R., Zhang, Y., & Zeng, J. (2011, July). Research on immunity-based intrusion detection technology for the Internet of Things. In 2011 Seventh International Conference on Natural Computation (Vol. 1, pp. 212-216). IEEE.

Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE Access, 7, 124379-124389.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.