Sabancı Üniversitesi

Duyarga Ağları ve Nesnelerin İnterneti- Güvenlik ve Mahremiyet

Prof. Dr. Albert Levi

Sabancı Üniversitesi
Bilgisayar Bilimi ve Mühendisliği

Albert Levi

- Doktora: Boğaziçi Üniversitesi, 1999
- Genel çalışma alanı bilgisayar ve ağ güvenliği
  - 2002 yılı başından beri Sabancı Üniversitesi
  - Oregon State University (1999 – 2002) ve Dalhousie University (2017 – 2018) ziyaretçi öğretim üyesi
- 6 destekli projede (TÜBİTAK, Santez, Sanayi destekli) yürütücü 3 projede araştırmacı.
- Değişik sanayi projelerinde danışmanlık (bazı projelerin bir kısmı alt yüklenici olarak üniversitede yapıldı)
- 100+ yayın
- 33 master ve doktora mezunu

Albert Levi – Araştırma Alanları Genel Bakış

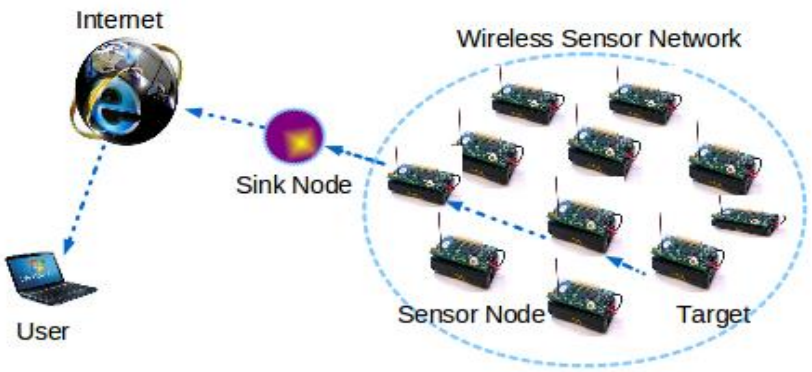
- Değişik ağ yapılarında güvenlik sorunları
  - Telsiz ağlar, duyarga ağları, gövde alan ağları, RFID, akıllı kartlar, ad hoc ağlar, nesnelerin internet, vs.
- Anahtar paylaşımı ve yönetimi
- Mahremiyeti korumalı sistemler
  - Mahremiyet korumalı IDS log paylaşımı
  - Duyarga ağlarında mahremiyet korumalı veri paylaşımı
  - Mahremiyet korumalı IoT kimliklendirme, otorizasyon ve güvenlik (devam etmekte olan proje)
  - Mahremiyet korumalı akıllı IoT atak tespiti (planlanan proje)

Anahtar Paylaşımı

- Duyarga ağları ve IoT sistemlerinde düşük maliyetli kriptografik anahtar paylaştırma
  - Önceden birbirini tanımayan ekipmanlar arasında

- Üretim aşamasında jenerik cihazlar
- Sahada birbirlerini güvenli bir şekilde tanıyabilme yeteneği
- 2 TÜBİTAK projesi tamamlandı, 20+ yayın.

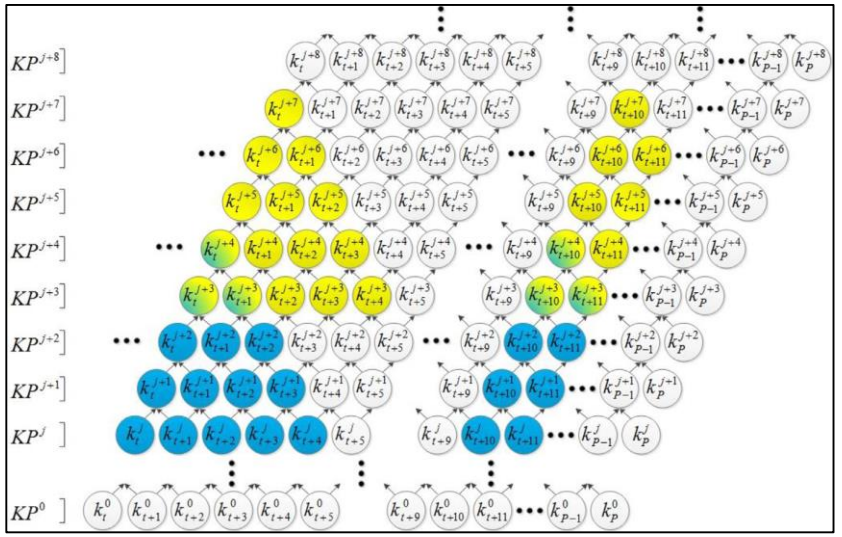
- Genelde öndağıtımlı ve ölçeklenebilir modeller kullanıldı
- Sonradan IoT'ye de adapte edildi

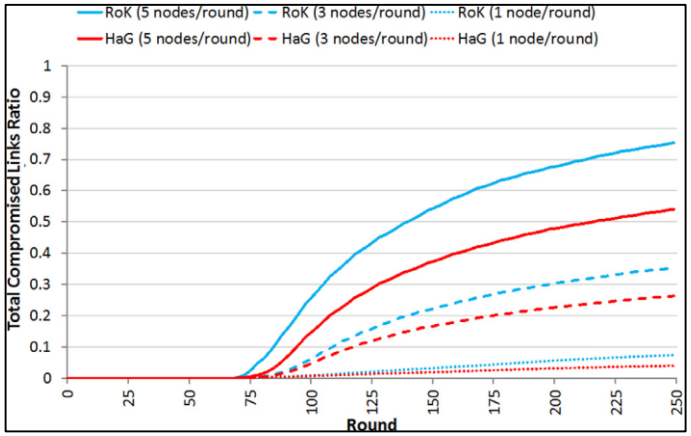


IoT Cihazları Arası Anahtar Paylaşımı

- Duyarga ağları için yapılan çalışmalar IoT sistemine uyarlandı

- *HaG: Hash Graph model*: anahtar havuzları nesiller halinde yenileniyor
  - Önceki nesillerle bağlantılı bir şekilde
  - Anahtarlar yenileniyor
- Geçici ataklar zaman içinde kendi kendine etkisini yitiriyor → sürdürülebilir güvenlik
- Mobiliteyi destekleyen bir sistem
- %90 ve üzeri bağlanırlık
- Rakip mekanizmalara göre hafif ataklarda %50, ağır ataklarda %10 daha iyi dayanıklılık sağlıyor

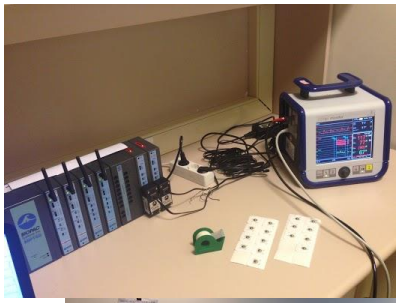




- A. Levi and S. Sarımurat, "Utilizing Hash Graphs for Key Distribution for Mobile and Replaceable Interconnected Sensors in the IoT Context", Ad Hoc Networks, vol. 57, pp. 3-18, Elsevier, DOI: 10.1016/j.adhoc.2016.08.013, March 2017.

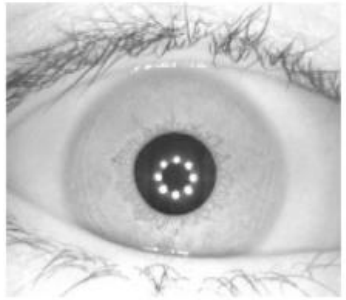
Gövde Alan Ağlarında Anahtar Paylaşımı

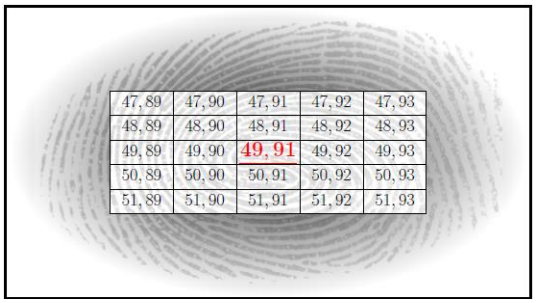
- 2015- 2017; TÜBİTAK 1001 projesi
  - 1 doktora, 3 y.lisans öğrencisi
  - 12 yayın
- Fizyolojik sinyallerinden yüksek entropiye sahip kişiye özel kriptografik anahtar üretilebileceğini gösterdik.
- EKG (Elektrokardiyogram) , PPG (Fotopletismogram) ve kan basıncı değerlerinden türetilen ortak metriklerle çalışıldı.
- Böylece vücudun farklı yerlerinden edinilen sinyallerle aynı kriptografik anahtarın üretilebileceği gösterildi.
  - Zaman ekseninde farklılaşma: anahtarların zaman içinde değişimi için önemli
  - Kişiler arasında farklılaşma: kimlik hırsızlığını önlemek için önemli
- Laboratuvar ortamında gönüllerden kendi fizyolojik veri bankamızı oluşturduk.
- Benzer çalışmaları biyometriden anahtar üretimi için de yaptık.



Biyometrik Veriden Anahtar Oluşturma

- Kimlik doğrulama amaçlı endüstriyel uygulamalar var
- Test ve şablon verisi arasındaki en küçük fark dahi biyometrik veriyi kriptografik anahtar olarak kullanmaya engel
  - Literatürdeki yöntemler hata düzeltme kodları ve/veya anahtarı biyometrik ile gizlemeye yönelik
- Bizim yaklaşımımız doğrudan biyometrik veriden anahtarı her iki tarafta da üretebilmek
  - En düşük masraflı alternatiften başlayarak olası anahtarları akıllı bir şekilde deneyerek ilerleyen güvenli bir protokol
    - Niceleme yoluyla alternatifleri azaltma
    - Sahte veri ekleyerek güvenlik ve mahremiyeti azaltma
  - İris ve parmak izi biyometriğine ayrı ayrı uyarlandı
- Parmak izi versiyonu
  - %99'un üzerinde doğru anahtar oluşturma oranı
  - %1'in altında hatalı anahtar oluşturma oranı
  - 96-bit anahtar güvenliği

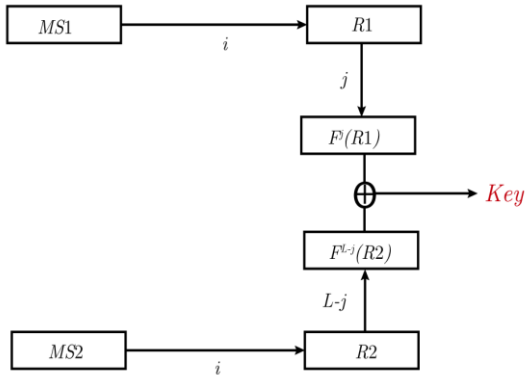


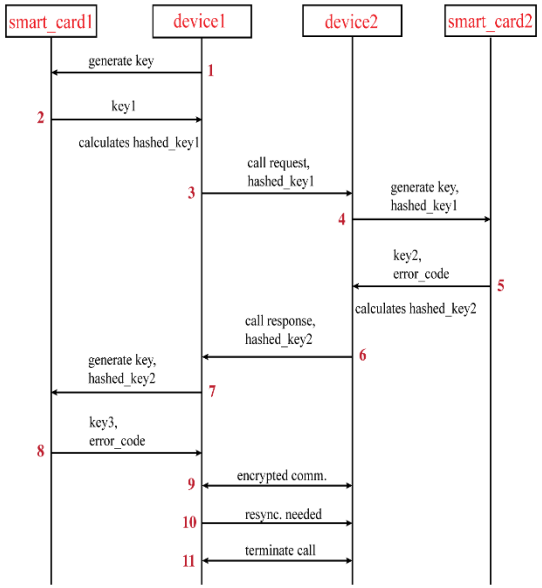


- İris versiyonunda kullandığımız veri setinde %100 doğru anahtar, %0 yanlış anahtar oluşturma oranı ve 127-bitlik güvenlik

Güvenli Multimedya İletişimi için Tek Kullanımlı Anahtar Üretimi

- Netaş ve Uludağ Üniversitesi ile birlikte yapılan SANTEZ projesi
- Eş kullanıcılar arası çoklu ortam iletişimi için oturum bazlı
periyodik anahtar değişimi
  - Akıllı kartlar üzerinde uygulandı
  - Özet zinciri kavramı
  - Her iki tarafta da senkron bir şekilde aynı anahtarın sadece özet operasyonları ile oluşturulması
  - İleri ve geri gizliliği sağlıyor
- Çağrı başlangıcındaki sinyalleşme sırasında anahtar doğrulanarak olası senkronizasyon sorunları engelleniyor
- Değişik akıllı kartlarda denendi ve sanayi ortağı kurumun
ürününe uygulandı





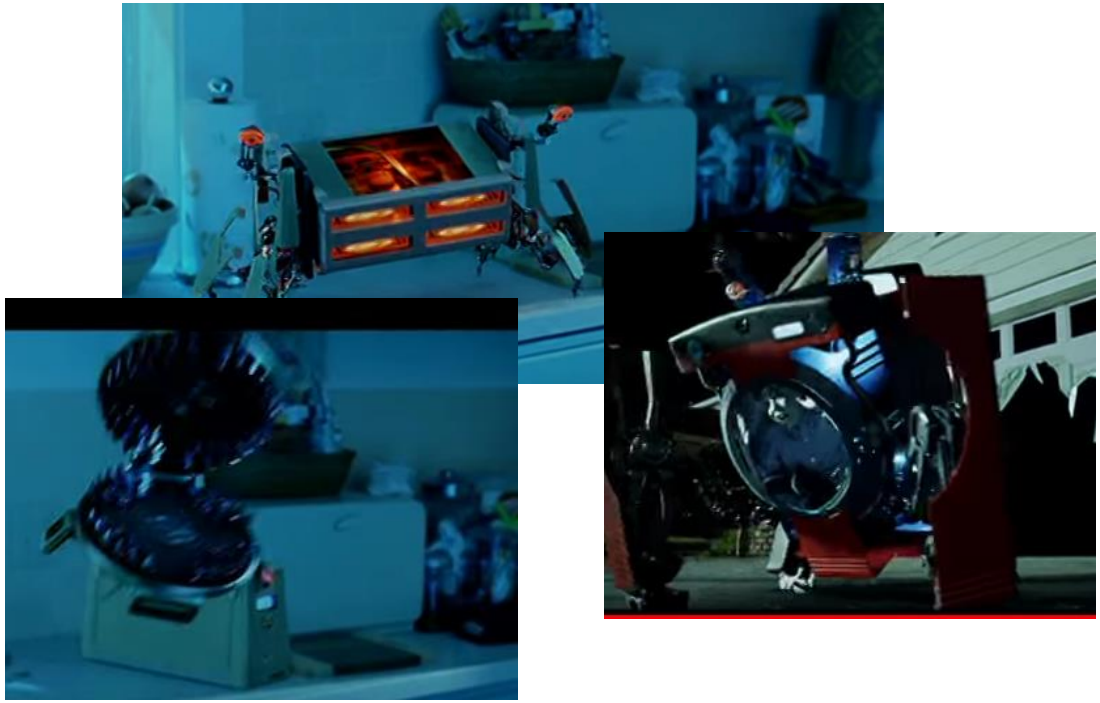
- Ö. M. Candan, A. Levi and C. Togay, "Generating one-time keys for secure multimedia communication", in Proceedings of 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, 2018,

Güncel IoT Güvenliği/Mahremiyet Sorunları

- Asıllama, Gizlilik, Bütünlük
  - Hem kullanıcı hem de veri odaklı
  - Çoğunlukla uygulamadan bağımız
  - Çözümler büyük oranda kriptografik
- Ağ tabanlı ataklara karşı dayanıklılık ve direnç
  - Ağ katman atakları
    - Duyarga ağları RFID dünyasından miras kalan ataklar
    - Yol atama protokollerini hedef alan ataklar, ağı anlamsız kontrol mesajları ile tıkama, kara delik atakları, vs.
  - Kötücül yazılımlar, botnetler, DoS atakları, sızma
    - Eski kavramlar ama IoT dünyasına özelleşmiş durumdalar

Yakın bir Vaka – Mirai Botnet (2016)

- Bir milyon civarında IoT cihazının ele geçirilip bot olarak kullanıldığı bir DDoS atağı
- Elbette Hollywood daha önce bunu öngörmüştü (2009 tarihli G-force filmi)



Mirai Botnet

- IoT cihazlarından oluşan botnet bir DNS sağlayıcısına (Dyn) saldırarak yıkıcı bir tıkanıklık oluşturdu
- Çoğunlukla IP kameralar ele geçirilip bot olarak kullanılmıştı.
- Milyonlarca kişinin İnternet erişimi sekteye uğradı.

- Neden oldu?
  - Varsayılan şifreler → cihazların ele geçirilmesi çok kolay
  - Cihazların arasında veri iletişimi
    - Çoğunlukla açık, kimlik doğrulamasız
    - Güvensiz → şifreli ve kimlik doğrulamalı bile olsa ele geçirilen bir cihazdan gelen verinin doğruluğunu kontrol edecek bir mekanizma yok
- Çıkarılan ders
  - Şifreleme, TLS: içeriğe güven duymanız için yeterli değil
  - Asıllama, OAuth2.0: cihaza güven duymanız için yeterli değil
  - Kötücül yazılımlar, oltalama atakları vs. için içeriğin akıllı bir şekilde analizi gerekiyor → makine öğrenmesi

Makine Öğrenmesi ile IoT Atak Tespiti

- Benzetim ile (Contiki OS – Cooja Simülatörü) veri seti
- 3 farklı atağı çoklu sınıflandırma ile %99 kesinlikle tespit edebildik
- Veri modelimiz saldırgan düğümün kimliğini de tespit edebilmekte

Validation Accuracy: 0.9904988123515439

	precision	recall	f1-score	support
0	0.97	1.00	0.98	624
1	1.00	0.97	0.98	663
2	1.00	1.00	1.00	627
3	1.00	1.00	1.00	612

Validation Confusion matrix:

```
[[622   2   0   0]
 [ 22 641   0   0]
 [  0   0 627   0]
 [  0   0   0 612]]
```

Test Accuracy: 0.9924782264449723

	precision	recall	f1-score	support
0	0.97	1.00	0.99	626
1	1.00	0.97	0.98	629
2	1.00	1.00	1.00	649
3	1.00	1.00	1.00	622

Test Confusion matrix:

```
[[626   0   0   0]
 [ 19 610   0   0]
 [  0   0 649   0]
 [  0   0   0 622]]
```

Teşekkürler

Albert Levi
Sabancı Üniversitesi
levi@sabanciuniv.edu