



Bezvadu ierīču modeļu noteikšana

Maģistra kursa darbs

Autors: **Aija Kraševska**

Stud.apl.nr: ak11027

Darba vadītājs: Dr.sc.comp. **Pēteris Paikens**

Problēma:

Augot bezvadu ierīču skaitam un dažādībai, aug iespējas ļaunprātīgai bezvadu sakaru protokolu izmantošanai. Apkārt esošo aktīvo bezvadu ierīču atpazīšana ir pirmais solis ievainojamību atklāšanā.

Mērķi:

1. Noskaidrot šobrīd praksē lietotās modeļu noteikšanas metodes.
2. Noskaidrot ierīču noteikšanas iespējas dažādos OSI līmeņos.
3. Sniegt rekomendācijas efektīvākajām ierīču atpazīšanas metodēm.

OSI slānis	Atribūti
Lietotnes slānis (7. līmenis)	GATT pieejamā STRING kopa GATT pakalpojumu kopa Ierīces izmantotie protokoli
Transporta slānis (4.līmenis)	Datu sūtīšanas biežums Izmantoto pakalpojumu kopa
Tīkla slānis (3. līmenis)	IP adrese
Datu posmu slānis (2.līmenis)	MAC adrese
Fiziskais slānis (1. līmenis)	Radio frekvence Sūtīto datu apjoms Sūtīto datu aina Sūtīto datu nesējfrekvences nobīde Ierīces aktīvais un pauzes laiks

Ietvara nosaukums	Bezvada savienojuma veids	Algoritma precizitāte
A.Sivanathan 2017	WiFi	95%
Vispārīgo atribūtu profils (GATT)	Zemas jaudas Bluetooth	Pakalpojumiem: 99.7%
		Iezīmēm: 99.96%
BLE SDR	Bluetooth	99.8%

Secinājumi:

- Katram bezvadu protokolam ir noteikti iekšējie protokoli un arhitektūra.
- Viena iekārta var izmantot vairāk nekā vienu bezvadu protokolu.
- Zemākajos OSI līmeņos ierīces atribūtu kopu ievāc ar pasīvo metodi
- Mašīnmācīšanās ir efektīva ierīču noteikšanas pieeja.
- Darbā apskatīti vairāki ierīču atpazīšanas ietvari, kuru precizitāte vismaz 95%
- Universāls ietvars nepastāv.
- Atribūtu kopu var iedalīt grupās pēc dažādām īpašībām.

Turpinājums:

- Analizēt citus bezvadu protokolu atpazīšanas ietvarus
- Paplašināt atribūtu sarakstu
- Izpētīt aktīvās datu ievākšanas metodes
- Pielietot un modificēt atrastos ietvarus