

Drošība, Privātums, Uzticamība

Uldis Bojārs

Datorikas fakultāte
Latvijas Universitāte

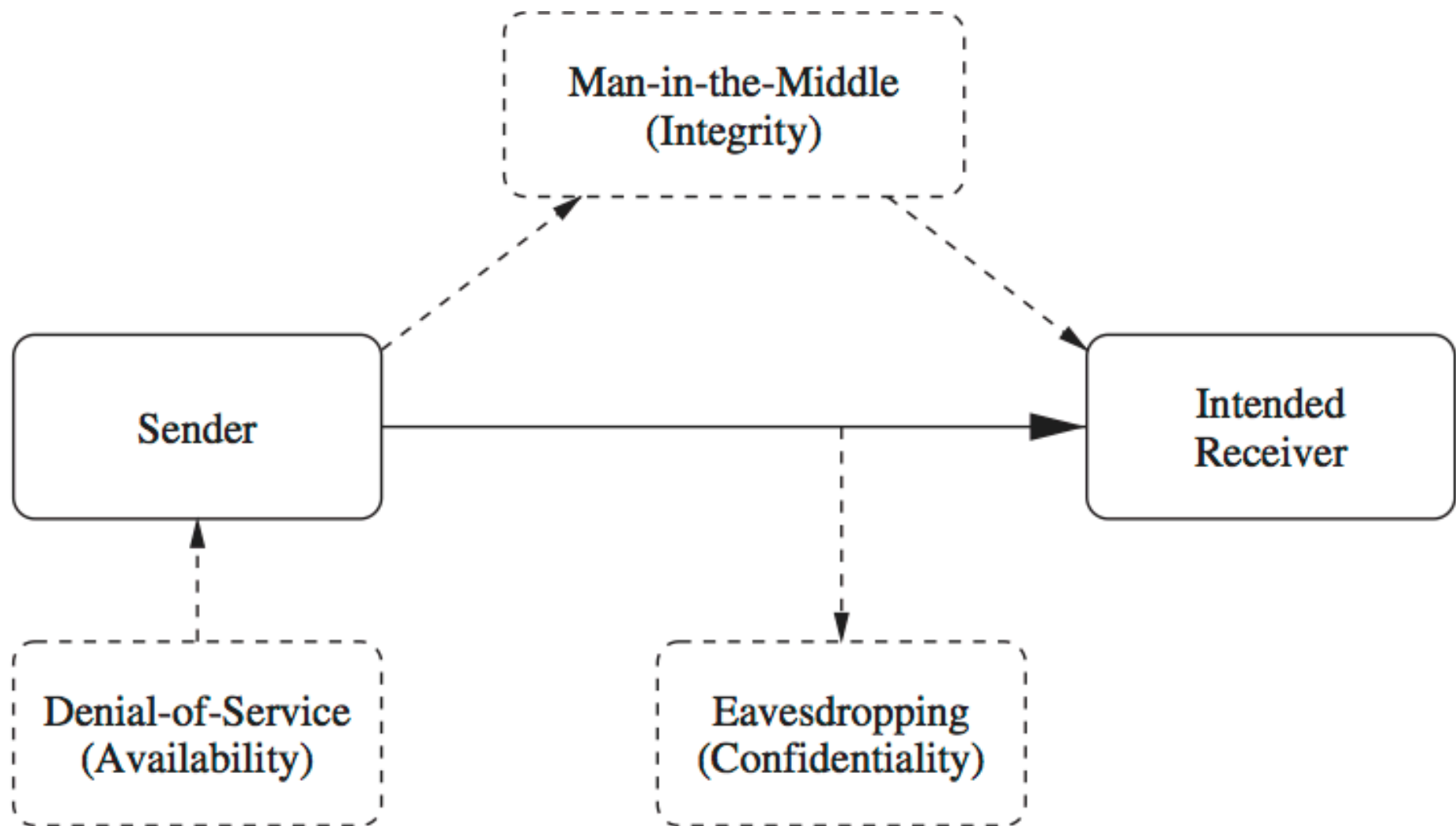
06.nov.2013.

Ievads

- Sensoru tīkli nav unikāli, frekvences un modulācijas metodes ir standartizētas, ikviens var atkārtot mūsu darbības
- Bezvadu savienojumi daudz ievainojamāki
- Arī interneta pirmsākumos neviens nedomāja, ka kādam ienāks prātā veikt kaitniecību

CIA “trijotne”

- Confidentiality
- Integrity
- Authenticity



CIA model: Examples of attacks.

Fundamentals of Wireless Sensor Networks. W.Dargie, C.Poellabauer. Wiley, 2010.

Sensoru tīklu specifika

- Ierobežoti resursi
 - grūtības lietot drošības mehānismus, kas prasa daudz resursus vai regulāru komunikāciju ar citām ierīcēm
- Tīkli [daļā gadījumā] liela izmēra, decentralizēti
- Darbojas nomaļās vietās, nepieskatīti
- Komunikācija nav uzticama, var būt kļūdas
 - kā atšķirt uzbrukumu no aparatūras kļūdām?

Uzbrukumi dažādos līmeņos

- Uzbrukumi iespējami pilnīgi visos “OSI līmeņos”:
 - Fiziskajā (Physical)
 - Kanālu (Data Link)
 - Tīkla (Network)
 - Transporta (Transport)
 - Aplikācijas (Application)

Fiziskais līmenis, uzdevums

- Fiziskajā līmenī sensoru tīkla uzdevums ir:
 - Taupīt enerģiju
 - Izmantot radio ēteru efektīvi
 - Glabāt droši slepenu informāciju (atslēgas)
 - Izmantot kriptogrāfiju, ja nepieciešams

Fiziskais līmenis, problēmas

- Problēma 1 - Fiziska piekļuve mezglam dod iespēju nolasīt un izmainīt pilnīgi visus datus, tai skaitā, atslēgas
- Risinājums 1: droši korpusi – dārgi (neatbilst sensoru tīklu prasībai: mazi un lēti)
- Risinājums 2: Sensoru mezgls mēģina identificēt, ka tas tiek “nozagts” un šādā gadījumā izdzēš visus datus
- Problēma 2 - Radio signāla traucējumi (RF Jamming):
 - Pārtrauc savienojumu starp motēm
 - Rosina pārmērīgu komunikāciju ar mērķi iztērēt pēc iespējas vairāk enerģijas tīkla mezgliem
- Risinājums: identificēt un ignorēt traucētos apgabalus

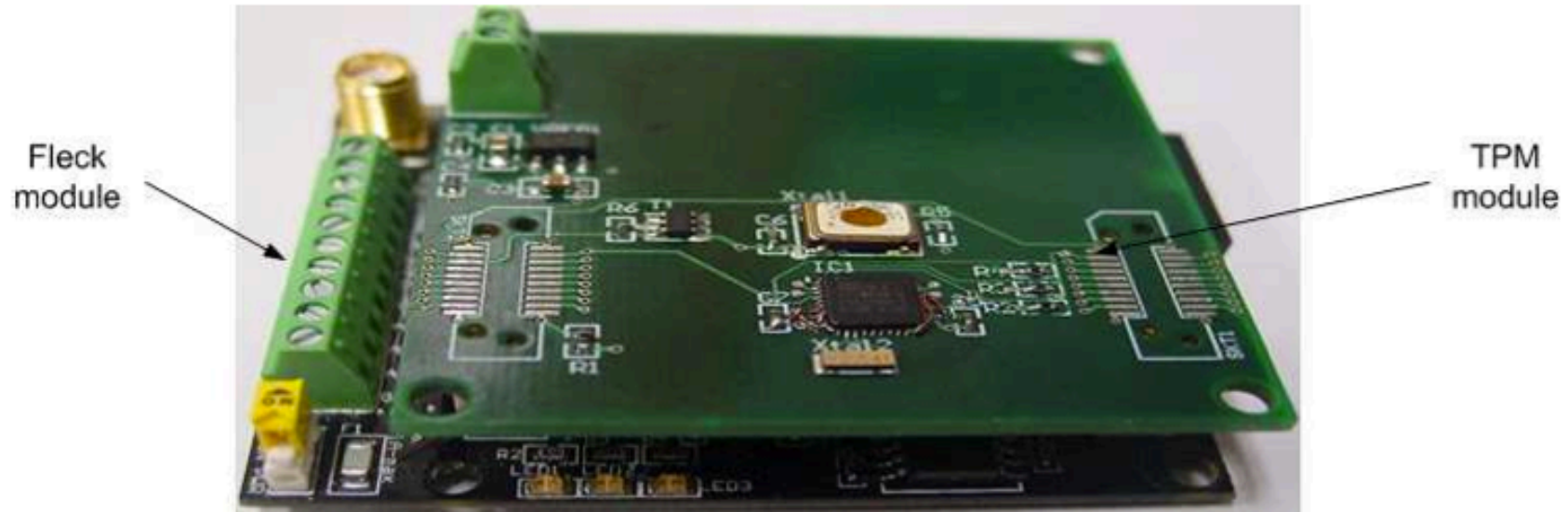
Fiziskais līmenis, atslēgas

- Problēma 3: kā inicializēt šifrēšanai izmantotās atslēgas tīklā?
- Risinājums 1: Aprīkot visus mezglus ar vienotu atslēgu. Slikti: katrs mezgls var “nodot” visus pārējos
- Risinājums 2: Izmantot čipā “iededzinātas” atslēgas
- Risinājums 3: Izmantot noslēgtu telpu katram sensoru mezglu pārim atslēgu inicializācijas brīdī

W.C.Shih, W. Hu, P. Corke, L. Overs. *secfleck: A public key technology platform for wireless sensor networks*

C.Kuo, M.Luk, R.Negi, A.Perrig, *Message-In-a-Bottle: User-Friendly and Secure Key Deployment for Sensor Nodes*

Hardware šifrēšanas modulis



W.C.Shih, W. Hu, P. Corke, L. Overs.
secfleck: A public key technology platform for wireless sensor networks.
Wireless Sensor Networks, Springer, 2009.

Fiziskais līmenis, atkārtošana

- Problēma 4: Ja iebrucējs noklausās ziņojumu, iespējama šī ziņojuma atkārtota nosūtīšana
- Risinājums 1: Izmantot augošu skaitītāju, ko pievieno katrai paketei
- Risinājums 2: mainīt atslēgas laika gaitā
- Problēma 5: kriptogrāfijai nepieciešami resursi un laiks
- Risinājums 1: specializēti kriptogrāfijas čipi
- Risinājums 2: vienkāršāk rēķināmi algoritmi

Kanālu līmenis, uzdevums

- Kanālu līmenī sensoru tīkla uzdevums:
 - Nodrošināt radio ētera efektīvu sadali visiem mezgliem, ņemot vērā individuālos un kopējos enerģijas resursus
 - Novērst kolīzijas
 - Nodrošināt efektīvu komunikācijas vadītāja lomas sadali

Kanālu līmenis, problēmas

- Problēma 6: Komunikācijas vadītājs ir vājš punkts
- Risinājums: Periodiski mainīt vadītāja lomu starp mezgliem
- Problēma 7: Komunikācijas koordinēšanai jāapmainās ar ziņojumiem, kurus iespējams viltot
- Risinājums: Izmantot augošus skaitītājus
- Problēma 8: Skaitītāju uzturēšanai jāizmanto tabula, kurai nepieciešama atmiņa. Iespējams uzbrukums, kas aizpilda tabulu ar fiktīviem datiem
- Risinājums: Tabulā ierakstus likt tikai, autentificējot moti + pa laiku tabulu iztīrīt

Tīkla līmenis, uzdevums

- Tīkla līmenī sensoru tīkla uzdevums:
 - Nodrošināt mezglu adresāciju, relatīvu vai globālu
 - Nodrošināt maršrutizāciju, izmantojot laika un enerģijas resursus efektīvi

Tīkla līmenis, problēmas

- Problēma 9: Globālai adresācijai nepieciešami lieli adrešu intervāli, ar IPv4 par maz
- Risinājums 1: IPv6 (6lowpan)
- Risinājums 2: Relatīvā adresācija tīkla ietvaros
- Risinājums 3: Neizmanto adresāciju. Identificēt mezglus pēc datiem vai atrašanās vietas
- Problēma 10: Vairumā gadījumu tīklā ir centrālā bāzes stacija (sink), kas savāc visus datus, tā ir vājā vieta
- Risinājums: Sūtīt maldīgus ziņojumus no citiem mezgliem, kas traucē identificēt bāzes staciju

Tīkla līmenis, datu savākšana

- Problēma 11: Visus datus no sensora uz bāzes staciju pārraidīt dārgi, bieži vien fiziski neiespējami
- Risinājums 1: Veikt agregāciju
- Risinājums 2: Sensoru tīkls kā datu bāze, kas prot apstrādāt vaicājumus (TinyDB, Cougar)

Tīkla līmenis, maršrutizācija

- Problēma 12: Kaitnieki var iejaukties maršrutizācijā, novest datu plūsmu pa garākiem ceļiem, izveidot bezgalīgos ciklus vai ievest strupceļos
- Risinājums 1: Statiska maršrutizācija, ja tas iespējams
- Risinājums 2: Šifrēt maršrutizācijas ziņojumus
- Problēma 13: Kaitnieks, atrodoties uz optimālā ceļa, var noklausīties visus datus
- Risinājums 1: Mainīt maršrutus
- Risinājums 2: Šifrēt datus

Transporta līmenis, uzdevums

- Transporta līmenī, sensoru tīkla uzdevums:
 - Nodrošināt iespēju robežās datu nonākšanu līdz gala mērķim. Atšķirībā no TCP, netiek prasīta 100% droša piegāde un atskaites par katru ziņojumu
 - Nodrošināt kritisko ziņojumu nonākšanu gala mērķī ar maksimāli iespējamo varbūtību

Transporta līmenis, pārsūtīšana

- Problēma 14: Tiek pārsūtīti dati vairākās paketēs, vienas paketes pazušana nozīmē visu datu nederīgumu
- Risinājums: TCP līdzīgs mehānisms: skaitītāji katrai paketei, ja mezgli pa vidu starp sūtītāju un saņēmēju konstatē skaitītāja pārlēkšanu, pieprasa paketes pārsūtīšanu
- Problēma 15: Kaitnieki nepārtraukti pieprasa pakešu pārsūtīšanu
- Risinājums: Šifrēt skaitītāju, izmantot autentifikāciju

Transporta līmenis, citas problēmas

- Problēma 16: Veidojas tīkla sastrēgumi
- Risinājums: protokola līmenī dinamiski mainīt sensoru lasīšanas un datu sūtīšanas biežumu, atkarībā no tīkla topoloģijas un enerģijas resursiem
- Problēma 17: Tīklā tiek lietotas agregātfunkcijas AVG, MIN un MAX, bet uzrodas ļaundari, kas sūta galēji lielas vai galēji mazas vērtības, izbojājot statistiku
- Risinājums 1: Nemt nevis vidējo vērtību, bet mediānu
- Risinājums 2: Ignorēt 5% mazāko un 5% lielāko vērtību

Aplikācijas līmenis

- Aplikācijas līmenī, sensoru tīkla uzdevums:
 - Nodrošināt lietotāja saskarni. Sensoru tīkla lietotājs: pētnieks
 - Nodrošināt (attālinātu) tīkla pārvaldības mehānismu
 - Aizsargāt aplikācijas vienu no otras

Aplikācijas līmenis, pārvaldība

- Problēma 18: Atrasties sensoru tīkla teritorijā ne vienmēr ir iespējams, bet reizēm nepieciešams mainīt tīkla darbību, piemēram, pārtraukt mērījumus
- Risinājums: Bāzes stacija savienota ar laboratoriju (WiFi, 3G). Sensoru tīkls atbalsta pārvaldības protokolu
- Problēma 19 (pārklājas ar problēmu 10): Savācēj-mezgls (sink) ir vājš punkts
- Risinājums: Ģenerēt viltus ziņojumus no citiem mezgliem, neatklājot īsto savācēju

Drošība un TelosB motes

- CC2420 transīveris
 - DSSS (spread spectrum)
 - IEEE 802.15.4 = MAC līmeņa drošības funkcijas
 - autentifikācija un šifrēšana (AES, 128-bitu atslēgas)
- CC2420 datasheet
 - <http://www.ti.com/lit/ds/symlink/cc2420.pdf>
- TinyOS 2.x tutorial
 - http://tinyos.stanford.edu/tinyos-wiki/index.php/CC2420_Security_Tutorial

Secinājumi

- Daudz problēmu dažādos līmeņos
- Reizēm visas problēmas nevar atrisināt, jāizvēlas svarīgākais
- Ne vienmēr jāšifrē visi dati, reizēm pietiek šifrēt kādu daļu
- Jaudīgākas kriptogrāfijas izmantošanai pieejami specializēti čipi ar lielu (relatīvi pret sensoru mezgla procesoru) šifrēšanas jaudu

9. Eseja

Jums ķermenim ir pievienots sensoru tīkls, kas mēra dažādus rādītājus (pulss, spiediens) un periodiski nosūta datus ārstam un kādam tuvam radniekam.

Kādus drošības pasākumus Jūs veiktu?

Termiņš: 13.11.2010. 10:00

Kontroldarbs = nākošnedēļ

- **jānokārto sekmīgi (>39%)**
- 90min laika
- visas līdz tam laikam apskatītās tēmas
- materiālu izmantošana maksā -20%
- saturs:
 - *multiple-choice* jautājumi
 - īsi, tekstā atbildāmi jautājumi
 - radošais uzdevums: sensoru tīkla piemērs