改善VANET安全的工程挑戰

Vehicular ad-hoc network(VANET)

第**3**投影片

通信延遲短

高速傳輸

人類面對更多的反應時間

為了更先進的安全性和便利性

第**4**投影片

車載網路的危險警告並非設計來去直接控制車輛，因此不立即影響道路使用者

第**5,6**投影片

a) 通過阻止真實消息來禁用真實警告。(無線電干擾，阻斷式服務攻擊)

b) 通過發送虛假信息製造虛假警告，以及降低司機對這些應用程序的信任。

c) 通過發送虛假消息創建虛假警告，並為不道德的司機提供不公平的優勢。

d) 竊取 PII（個人身份信息），司機駕駛歷(eavesdrop 竊聽)

第**7~9**投影片

防護與安全機制

* 機構認證CA (certificates authority)

1. 只有受到機構認證的車輛才可發送訊息
2. 經過認證後，鄰近車輛可以輕鬆識別認證車輛傳送的訊息

* 撤銷清單Revolution Lists

1. 只對已經認證過的車輛有效
2. 機構或監視車輛不合法行為，回報加入清單並循環發送至所有車輛網路中

* 隱私保護機制

1. 匿名：訊息傳遞不應包含識別車輛的密鑰

2. 不可追溯性：相鄰節點之ID每天至少更新數次

3. 安全性/不可追溯性:訊息日誌應該被安全存儲，一旦公開也不該被濫用

第**10**投影片

Long term / short term security mechanism :

長期安全機制: 不需要來回驗證，只需要一次

短期安全機制: 需要透過長期安全機制下的金鑰去加密得到

第**11**張投影片(安全機制面臨的挑戰)

* 上述VANET上的安全機制需要集中的通信網絡
* 安全與保障之間的權衡

例如，在機場，加強行李安檢和搜身等安全措施可能會提高安全性，但也可能會降低旅行效率並增加乘客通過安檢所需的時間。 在這種情況下，需要在安全性和安全性之間進行權衡，重要的是要取得平衡以確保適當地解決安全性和安全性問題。

* 加密、解密和認證性能(performance性能):時間花費與消耗資源多寡
* 物理攻擊
* 侵犯隱私權

第12張投影片

DLT((Distributed Ledger Technologies)分佈式帳本技術(去中心化，不可竄改性)

在區塊鏈上能儲存與管理個人分類帳上的動態個人交易，預防雙倍開支或是在沒有中央集權的非法交易(一個區塊包含一組交易，創建相互鏈接的區塊鏈)

第13張投影片

區塊鏈技術過程(last step 永久記錄，不可被撤銷)

第14張投影片(區塊鏈未來潛力與發展)

* 製造與物流:

能夠大量存儲，並且有保存性不需要過多操作，且去中心化

可以記錄位置/日期/位置/運輸負責人

* 維護和檢查:

可以記錄維修歷史，送檢召回紀錄，近期多個作業事務

* 所有權:

查看保險範圍來作為所有權之延伸

* 金融方面:

共享汽機車/通行費/電子交易/行動支付/停車費

第15張投影片

自製表格:說明比較優缺點

未來要結合VANET 跟 Blockchain會遇到的問題

* 頻繁網路拓樸(第16張投影片)

1. 如果我們將VANET的中心化授權取消，改由使用分散式安全機制去同步車輛，會導致VANET去中心化的優勢不再，也就是不再需要網路架構了
2. 若沒有涵蓋式的集中式網路，當有車輛離開或加入受限於通訊範圍

* 共識過程(創造區塊鏈時產生)

1. 個人參與者會透過創建新的區塊鏈來獲取虛擬貨幣作為獎勵
2. 我們不得不提出一個新的獎勵機制對於個人車輛希望創造新的 VANET區塊鏈通過消耗有限的計算性能板載微處理器。

因此需要調查VANET是否有足夠的帳本同步持續/延遲時間給予提供敏感安全程序

* 51% ISSUE

1. 前提在於大多數節點(車輛)屬於無惡意地，事實證明我們需要至少 51% 的合法車輛獲得安全共識過程。 然而一旦大量裝置有意無意地作惡，區塊鏈分佈可能被駭客利用來惡意更新。
2. 在一些共識過程中個別車輛的計算性能或帳戶狀態對共識過程的影響，我們需要小心惡意行為介入

* 隱私保護

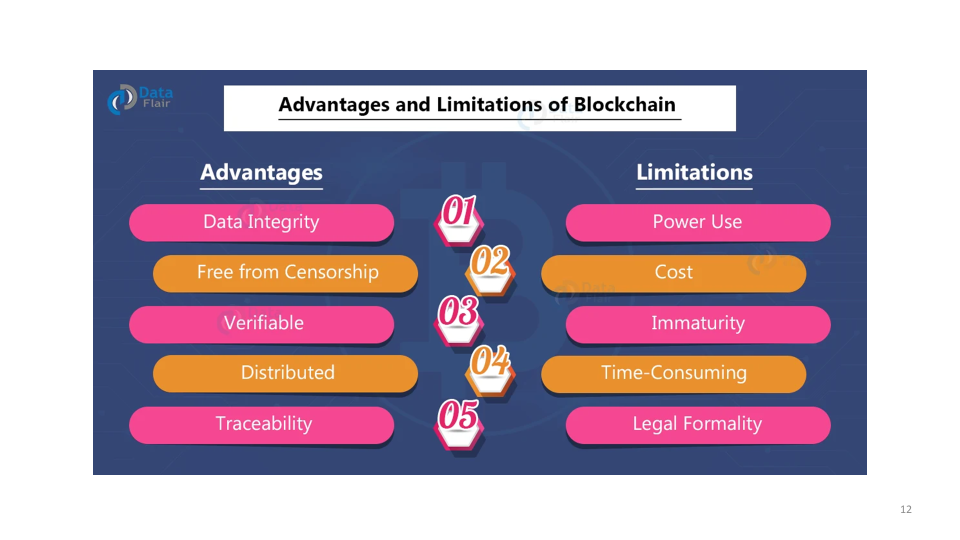
1. 駕駛歷程必須小心二次犯罪的濫用情形，我們需要合適的隱私防護機制，例如: long-term and short-term certificates

第16張投影片

最大的技術挑戰是目前提議的安全機制需要通信中心使認證機構和個人車輛交換訊息，例如:授權/安全密鑰

若這樣做，VANET 將失去其最大的優勢，不需要基地台來做交換

(vanet優勢:擁有中心基地台來做授權)

所以嘗試做出不需要基地台，依然可以認證彼此裝置的加密法則或機制。

(區塊鏈技術)