摘要

物聯網（IoT）設備由於其功能和能力的限制，容易受到眾多的安全威脅。在IoT中，由於電力有限的節點之間的無線通信通常呈間歇性。物聯網設備可能會被攝取，例如，導致節點重複攻擊的發生。

無線感測網絡（WSN）應該具備一種有效、準確和迅速的識別機制，可以察覺網絡中的干擾者和複製節點的存在。本文提出了一種基於支持向量機（SVM）的物聯網WSN克隆和干擾攻擊檢測技術。在這種技術中，基站（BS）通過檢查從物聯網設備到節點的距離測量，將節點分類為克隆或正常。模擬結果表明，所提出的SVM克隆具有高檢測準確性，並且具有降低的誤報率和能耗。

1.引言

物聯網（IoT）是一種發展中的網絡模型，包含大量相互連接的設備，彼此交互以便簡化人與物體之間的通信。例如，智能城市包含著眾多智能部門，如智能家居和智能醫院，它們是重要的IoT應用。在智能家居環境中，每個IoT設備都配備了內置的感測器和無線通信能力。這些感測器可以收集有關環境的數據，並與其他感測器、房屋所有者以及主要的監控系統進行通信[1]。許多IoT解決方案在成熟度上已有所發展。儘管能源消耗對整個網絡的壽命具有危險性，但這些設備還會遇到複雜的無線環境，影響具有極端變化能力的無線鏈路。這些所謂的低功耗損耗網絡（LLNs）利用各種解決方案以滿足最終用戶的需求。物理傳輸、媒介訪問控制和路由允許組織化的設備向收集、存儲和處理接收的數據的基站通知[2]。

由於其有限的功能和能力，IoT設備容易受到許多安全威脅的影響。在惡意干擾攻擊下，對數據安全的有效防護是一個重要但具有挑戰性的問題。在IoT中，無線通信通常在電力有限的節點之間進行間歇性地進行[3]。例如，IoT設備可能會被攝取，導致節點重複攻擊（也稱為克隆攻擊）。克隆攻擊非常具有破壞性，因為克隆設備將被視為具有真實身份的真實設備。這些克隆設備可以在網絡中輕松執行許多惡意行為，通過內部攻擊並插入虛假數據，從而引發IoT情境的危險[4, 5]。

在本文中，提出了一種基於支持向量機（SVM）的IoT WSN克隆和干擾攻擊檢測技術。

1.1 本工作的提出貢獻

所提出的克隆和干擾攻擊檢測的貢獻列舉如下：

i. 基於感測器節點的概率分佈，從網絡中選擇一個監控節點。

ii. 基站（BS）通過節點之間的成對距離確定節點的坐標。

iii. 基站定期執行SVM算法，基於測量的距離和扭曲閾值來檢測克隆攻擊。

iv. 為了避免虛假陽性，再次由監控節點對分類的節點進行交叉驗證，以確認克隆攻擊。

2 相關工作

Verma等人[6]對無線個人區域網絡（WPAN）網絡上的多種路由攻擊的結果進行了研究。從實驗結果可以看出，路由攻擊嚴重干擾網絡性能。因此，針對IoT網絡的不斷增加的攻擊可能會影響智能設備的整個網絡。他們設計了一個能夠感知所有路由攻擊的防禦系統。Lee等人[7]提出了一種基於多維尺度（MDS）的新的克隆識別技術，稱為**MDS clone**。**它似乎非常適用於IoT環境**，因為它（i）能夠在無需查找節點位置的情況下檢測克隆，並且（ii）與以前的方法不同，它可以應用於同時包含靜態和移動節點的混合網絡，其中不能事先假定沒有運動設計。Laguduva等人[8]引入了一種基於機器學習的有效方法，用於克隆強PUFs。他們還提出了一種新的鑑別器模型，以高度自信地識別克隆和原始PUFs。他們還提出了一種基於搜索的方法，通過三種常見的機器學習模型來識別指定克隆PUF的理想模型。Tedeschi等人[9]介紹了一種新的端到端安全設計方法，用於在改進製造設備的同時提供物聯網連接，以實現對傳統製造設備進行實時情況監控。該方法考慮了最佳實踐和指南，提出了一種新的領域特定方法，有助於彌合在車間引入IoT連接和保護系統和運營完整性之間的差距。Rausch等人[10]提出了一種點對點方法，通過強制網格網絡的拓撲結構來感知和限制這些對手。這樣做有三個主要好處。首先，他們提供了在真實智能電表部署中使用的IoT平台上的初始執行的視野。其次，他們提出了一種理想的對等節點選擇，可以幫助感知被干擾的節點，同時減小風險。

Haseeb等人[11]在移動IoT設備中實施了一個數據保護框架。它使用兩個函數以提供更好的安全性並降低能量消耗。然而，性能未在實時環境中進行分析。在[12]中，使用了一種混合方法進行特徵選擇，其中過濾方法的輸出被用作包裝方法的輸入，以提高分類器的性能。在過濾方法中，根據過濾模型選擇候選子集，在包裝方法中，使用分類器模型評估過濾模型。在這項工作中，使用了k-NN和RF分類器。Srividya和Devi [13]提出了一種基於多策略信任指標的WSN入侵檢測系統。通過使用三種信任指標，它識別了惡意節點和數據傳輸的最佳路徑。在AI-HydRa [14]中，設計了一個基於機器學習的混合決策模型，以在減少虛假陽性的同時獲得高檢測準確性。它結合了RF和深度學習（DL）模型來區分惡意文件和良性文件。

3 提出的解決方案

在本文中，提出了一種基於支持向量機的物聯網（IoT）無線感測網絡（WSN）的克隆和干擾攻擊檢測解決方案。在這項工作中，基站（BS）通過檢查從IoT設備到節點的距離測量，將節點分類為克隆或正常。首先，根據感測器節點的概率分佈，從網絡中選擇一個監控節點。基站定期執行SVM算法，基於節點之間的距離和失真閾值來檢測克隆攻擊。

3.1 系統模型

考慮了一個基於IoT的WSN，其中包含帶有基站（BS）的靜態和移動節點。每個感測器在每個時間段測量與其鄰近節點的距離並將詳細信息傳輸給基站。由於IoT節點的移動模式是不可預測的，移動節點會以隨機方向動態移動。在本文中，我們考慮一個能夠執行“克隆攻擊”的對手。他們能夠構建被捕獲的設備並將真實身份從被捕獲的設備存儲在眾多虛構的設備內。具體而言，我們應對的是克隆攻擊，其中在網絡中存在具有相同ID的多個受影響節點。

3.2 監控概率

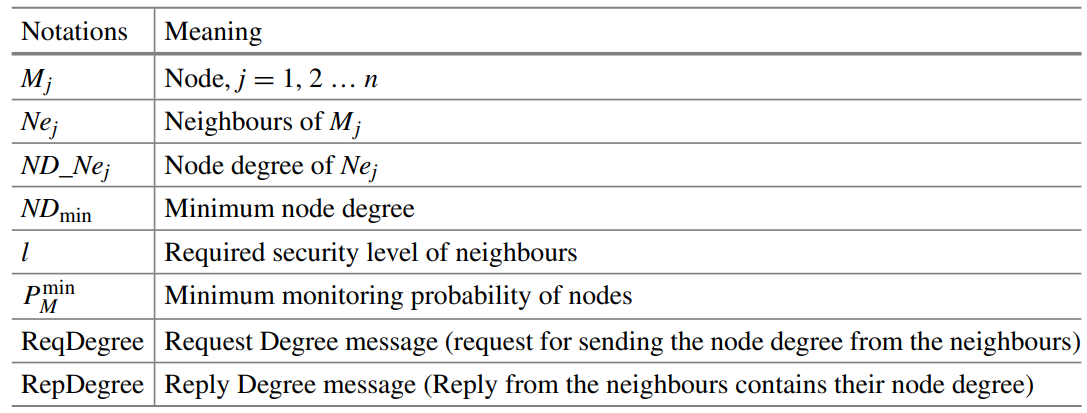
在這項工作中，選擇一個監控節點來監控一組節點。為了選擇監控節點，考慮了感測器節點的概率分佈。節點a在安全級別l被監控的概率由以下公式給出：



我們將節點的度定義為其任何時間的相鄰節點的數量。讓mi表示節點Ni相鄰節點的最小度。

**最小監控概率（MMP）**確保網絡中的每個節點都在所需的**安全級別**上進行檢查。

每個節點用來定義MMP的方法由以下過程示範



節點, j = 1, 2, … n

Mj的鄰居

Nej的節點度

最小節點度

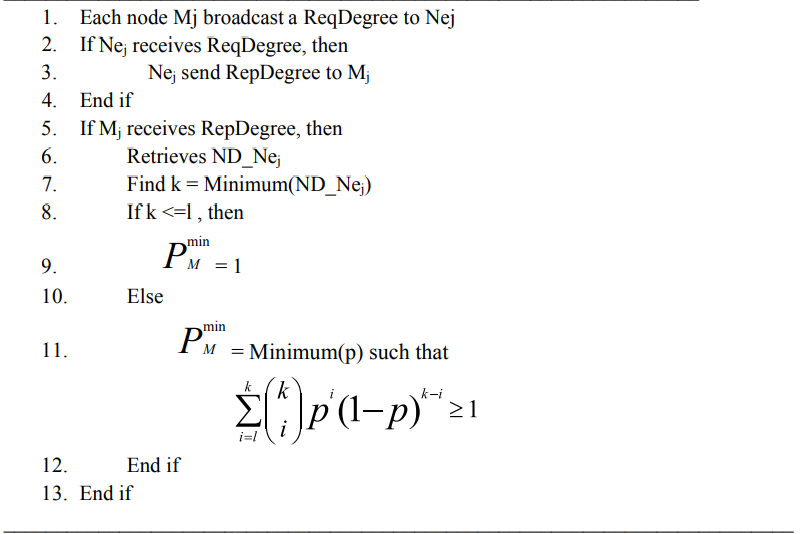
鄰居的所需安全等級

節點的最小監控概率

請求度消息

回復度消息

Algorithm – Monitoring Node Selection



1.每個節點 Mj 向其鄰居 Nej 廣播 ReqDegree。

2.如果 Nej 收到 ReqDegree，則

3.Nej 向 Mj 發送 RepDegree。

4.結束如果。

5.如果 Mj 收到 RepDegree，則

6.檢索 ND\_Nej。

7.找到 k = 最小值(ND\_Nej)。

8.如果 k <= l，則

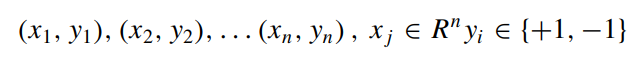
3.3 估算兩兩距離和定位

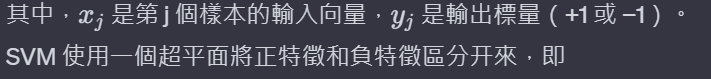
將距離矩陣DM視為輸入，其中包含所有節點對之間的距離。輸出是使用DM創建的一組坐標。每個節點計算與其相鄰節點的距離並將其通知給基站（BS）。然後，BS利用重建的節點位置來構建網絡地圖。BS通過這些步驟重複對兩兩距離進行DM的確定和執行定位。

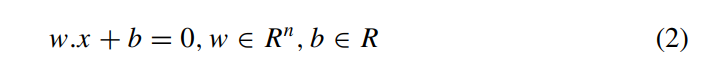
3.4 支持向量機（SVM）

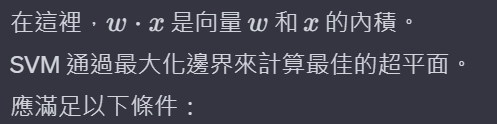
在介紹我們提出的克隆檢測技術之前，我們在本節提供了SVM的簡要背景，這將作為我們方法的基礎。考慮反映設備特性和與克隆和干擾攻擊相關的行為的特徵。與克隆攻擊相關的特徵包括：源和目標ID，它們的位置信息，與干擾攻擊相關的特徵包括通道響應，重發的RTS或數據，載波感測失敗率和網絡分配器向量（NAV）。

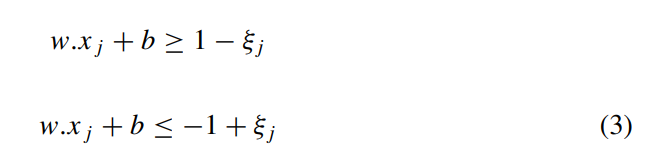
訓練集表示為：









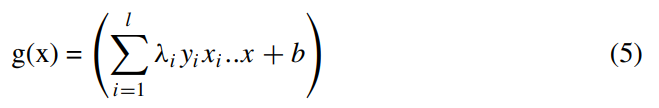


根據方程（2）的約束，方程（3）可以寫為



在這裡，C 是表示不滿足條件的成本的常數。

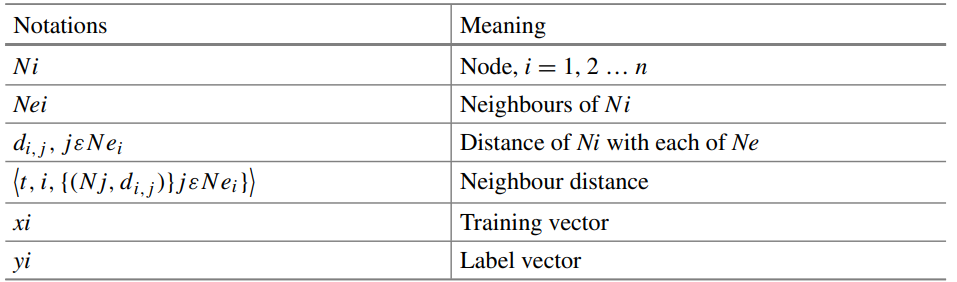
決策函數為



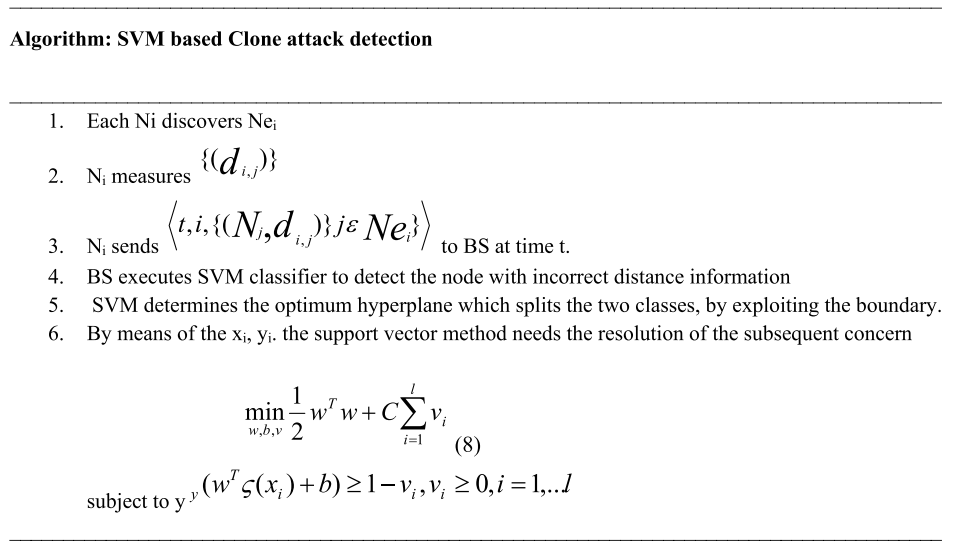


3.5 攻擊分類

基站執行以下算法來檢測網絡中是否存在克隆攻擊。



3. Ni 與每個 Ne 的距離



1.每個節點Ni在時間t向基站（BS）發送一個包含時間、節點ID和相鄰節點的距離信息的消息。

2.基站BS使用SVM分類器來檢測具有不正確距離信息的節點。

3.SVM確定最佳的超平面，將兩個類別區分開來，通過利用邊界。

4.通過xi和yi的平均值，支持向量方法需要解決相應的問題。

在攻擊分類中，基站通過傳送和接收距離查詢封包，獲得節點的一組兩兩距離。然後，通過使用三邊定位方法，基站評估等效節點的坐標。

3.6 由監控節點進行交叉驗證

為了避免將克隆節點錯誤地解釋為有效節點，監控節點需要對最初被認為是合法的節點進行二次檢查。

在監控節點收到來自基站的驗證請求後，它們通過檢查鄰居表中的節點ID和位置來驗證位置信息。如果存在衝突，那麼這些節點被確認為克隆節點。

4 實驗結果

提出的SVMClone技術在NS3中進行模擬，並與MDSClone [7]技術進行比較。實驗中使用的各種類型的感測器包括運動感測器和環境感測器。使用的各種IoT設備包括攝像機和智能手機。

4.1 結果與分析

在實驗評估中，攻擊間隔從20秒變化到100秒。

表1和圖1顯示了攻擊間隔變化時測得的受影響封包的百分比。由於SVMClone使用監控概率監控所有節點，因此在SVMClone的情況下，受影響封包的百分比比MDSClone少17%。

表1 受影響封包百分比的結果表

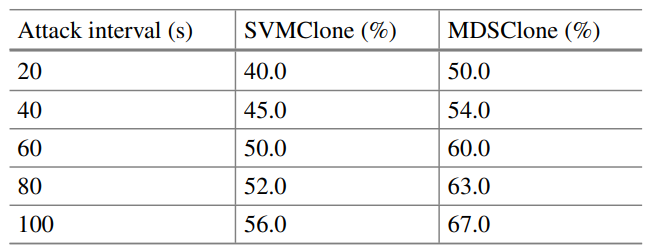


圖1 攻擊間隔的受影響封包百分比

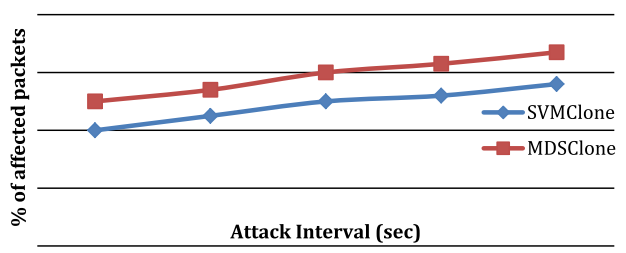


表2 檢測精度的結果表

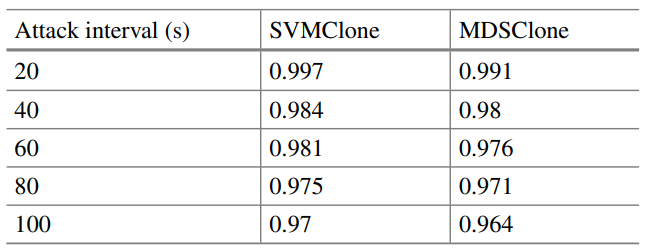


表2和圖2顯示了在攻擊間隔變化時測得的檢測精度。由於SVM增加了檢測的準確性，SVMClone的檢測精度比MDSClone高1%。

表3和圖3顯示了在攻擊間隔變化時的誤報率。由於監控節點的交叉驗證機制，SVMClone的誤報率比MDSClone低29%。

圖2 攻擊間隔的檢測精度

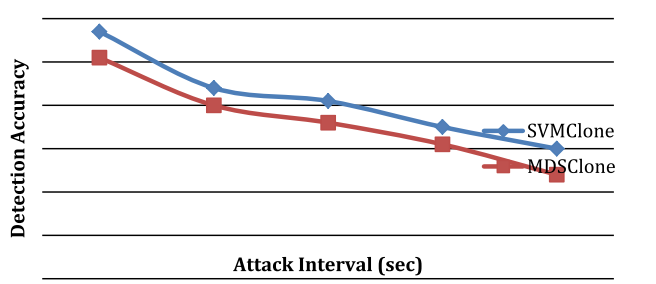


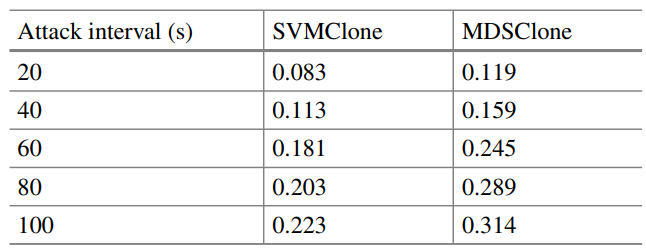
表3 誤報率的結果表

圖3 攻擊間隔的誤報率

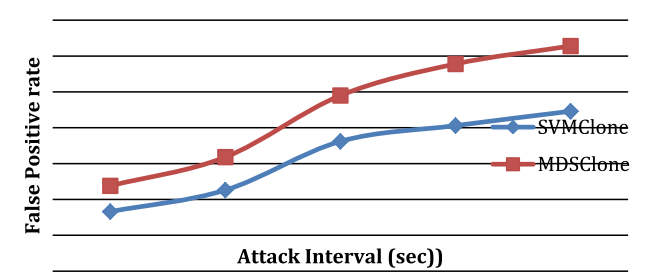


表4 殘餘能量的結果表

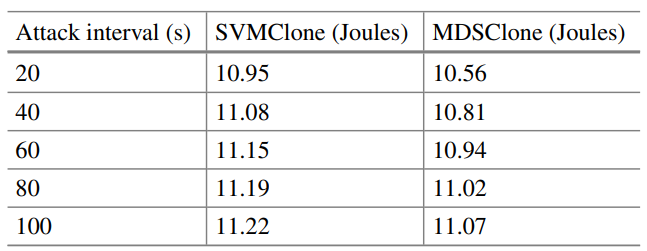


圖4 攻擊間隔的平均殘餘能量

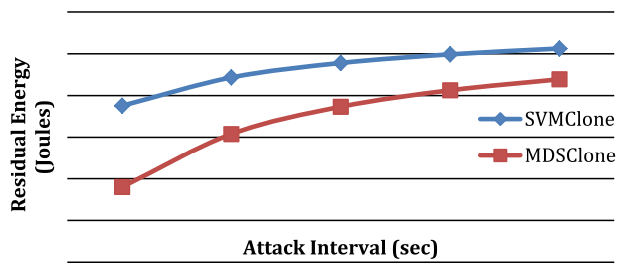


表4和圖4顯示了在攻擊間隔變化時的平均殘餘能量。由於SVMClone還消除了干擾攻擊，因此其殘餘能量比MDSClone高2%。

5 結論

本文提出了一種基於支持向量機（SVM）的物聯網無線感測器網路中克隆和干擾攻擊檢測的解決方案。在這項工作中，基站通過檢查來自物聯網設備的距離測量來將節點分為克隆或正常節點。

所提出的SVMClone技術已在NS3中進行了模擬，並與MDSClone技術進行了比較。模擬結果表明，SVMClone實現了高檢測精度，同時減少了誤報率和能耗。由於個人數據在物聯網應用（如智能家居網絡）中被收集並傳輸，安全和隱私問題變得越來越普遍，必須忽視這些問題，以充分利用智能家居環境。物聯網數據的隱私和安全性可能以多種方式受損。不受控制的設備可能基於信任濫用進行偏見攻擊。對物聯網對象的攻擊，特別是與信任有關的攻擊，是一種可能的攻擊。因此，未來的工作旨在提供保護隱私和防禦物聯網的基於信任的攻擊的解決方案。