適用於無線感測網路上動態金鑰管理協定

D0975253 資訊三丁 張詠翔

目錄

應用說明.................................................................................................................... 3

已知安全性問題.........................................................................................................4

運作方式.................................................................................................................... 5

預防攻擊.....................................................................................................................6

結論 ………………….….…..…..…………………………………………………………………………………….6

心得.............................................................................................................................6

應用說明:

在現今社會上，無線感測器的應用範圍非常的廣泛，像是利用無線感測器來去預防森林大火，雖然感測器的應用無遠弗屆，但是在限制上也有許多的不便，因為體積小，所以在電量 , 記憶體 , 運算能力等等...... ,皆被大大的限制住，即使有硬體上的限制，但是在實際應用上還是有著很不錯的表現。而在傳輸上，最引人擔憂的也就是網路的安全，為了能夠讓網路上的傳輸有著比較高的安全性，即需要使用秘密金鑰來進行感測器之間的通訊。在現今已經有著許多的金鑰建立的方法被設計出來，在大部分使用的金鑰算法中，最常被使用的就是從預先設立好的金鑰池中去挑選N把，形成一個金鑰鏈，每個感測在再金鑰鏈中去使用這些金鑰來進行加密，但是在傳輸秘密金鑰時，金鑰容易暴露在傳輸的過程中，導致內容可能會被修改,竊取，資料的安全性大大的降低，也有一些算法是對金鑰加密進行傳輸，但是對於運算能力受到很大限制的感測器，往往會導致感測器的壽命降低，也有不必要的資源消耗。為了解決金鑰傳輸上安全性的問題，所以提出動態金鑰管理的協定，來提高金鑰的安全性。透過動態的方式去更新金鑰，讓金鑰被猜中的機率大大的降低，也能避免感測器在網路上被攻擊的情況發生。

已知的安全問題:

在金鑰的傳輸上，對於將秘密金鑰進行傳輸的保護不夠安全，並且受到硬體的限制，導致演算法的運算不能太複雜，以免導致減少感測器的壽命和不必要的資源消耗，也因為如此金鑰有一定的機率被猜中，在資料隱密性,資料認證會有疑慮，也會受到中間人的攻擊,重送攻擊,資料竄改等等安全上的問題

解決問題的方式:

提出動態金鑰管理協定，利用叢聚的管理方式去進行資料的傳輸，在感測器的網路上，將眾多的感測器節點去劃分區域，讓感測器可在有效的範圍內進行傳輸，並有一個叢聚點的感測器來匯集各個感測器所傳來的資料。

運作方式:

1. 每個感測器會先被給予兩個參數，並且使用單向赫序函數方法來產生新的一把金鑰，透過所產生的金鑰來和叢聚節點溝通，並將預先配置用於加密通知各感測器節點更新金鑰的訊息金鑰和本身編號經由單向赫序函數產生的金鑰傳輸到叢聚點
2. 叢聚點將各個編號匯集成一個列表，並由叢聚點預先的2個參數製造一把金鑰，將列表,時間戳記和叢聚點編號加密傳送給基地台
3. 基地台確認叢聚點編號，從資料庫找出對應的金鑰解密，並透時間參數的運算，看是否有符合特定時間，如果沒有，則丟棄，反之，將列表的各個編號對應的金鑰做成一份新的列表，最後將新的列表,時間戳記使用叢聚點的金鑰進行加密，傳給該叢聚點
4. 叢聚點用同樣的方式對封包進行辨識，並更新自己的金鑰，也利用在第一步收到的訊息金鑰通知各個感測器更新金鑰，並傳送封包告知基地台進行資料庫資料的更新。
5. 各感測器將金鑰進行更新(利用舊的金鑰和原先的參數進行運算產生新的金鑰)

預防的攻擊:

1. 預防惡意猜測攻擊: 金鑰和資料庫經過一段時間會更新，使攻擊者無法得知金鑰，而每個節點最多紀錄三把金鑰，減少記憶體的空間
2. 預防重送:利用時間戳的運算方式來避免重送
3. 預防資料竄改攻擊: 叢聚點和感測器間利用金鑰加密，當叢聚點從資料庫拿到對應的金鑰列表，進行解密時，如果解不開則是為危險封包直接丟棄，可以確保資料的完整性

結論:

因為無線感測網路的一些限制，使用資料的批次溝通，來降低感測節點的秏電力，每個感測節點，最多只需要記錄三把金鑰，不需記錄整個金鑰鏈，此方法可有效的節省感知節點的記憶空間。

 每一次的傳輸中，所使用的金鑰都是只適用於此次的傳輸，下次要在傳輸時，所使用的金鑰又有所不同，這樣的方法可降低攻擊者去猜測出金鑰，進而提高它的安全性。

在傳輸方面，我們在每個傳輸的過程中，都使 用到記錄時間戳記，透過接收端和傳送端兩方 的計算，可確保預防重送攻擊的發生

心得:

在生活上很少去接觸到感測器網路的相關問題，經由這次的報告，也對於感測器的網路傳輸有了基本認識，尤其是對於使用在感測器上的演算法的一些利弊，得知了動態金鑰管理的原理與目的，也才了解到原來小小的感測器在經由網路傳輸時，有著諸多的不便，調解軟硬體之間的限制，去取得最佳做法，真的是蠻困難的，但儘管如此感測器在我們的生活上的應用真的非常的廣泛，也非常的重要。