

Securing Multi-Hop Wireless Networks Against Impersonation Attacks

Steve Glass (stephen.glass@nicta.com.au)
 NICTA Queensland Research Lab &
 Griffith University Institute for Integrated and Intelligent Systems

PROBLEM DEFINITION

Multi-hop wireless networks as used in sensor nets are particularly vulnerable to impersonation attacks. In this class of attacks a hostile adversary controls one or more nodes which misrepresent their identity and selectively forward traffic to legitimate recipients. Such attacks can be used to undermine network integrity, availability and reputation-based trust schemes. We are investigating both middleperson (also known as man-in-the-middle) and wormhole attacks[1] (a wormhole attack is illustrated in figure 1 below)

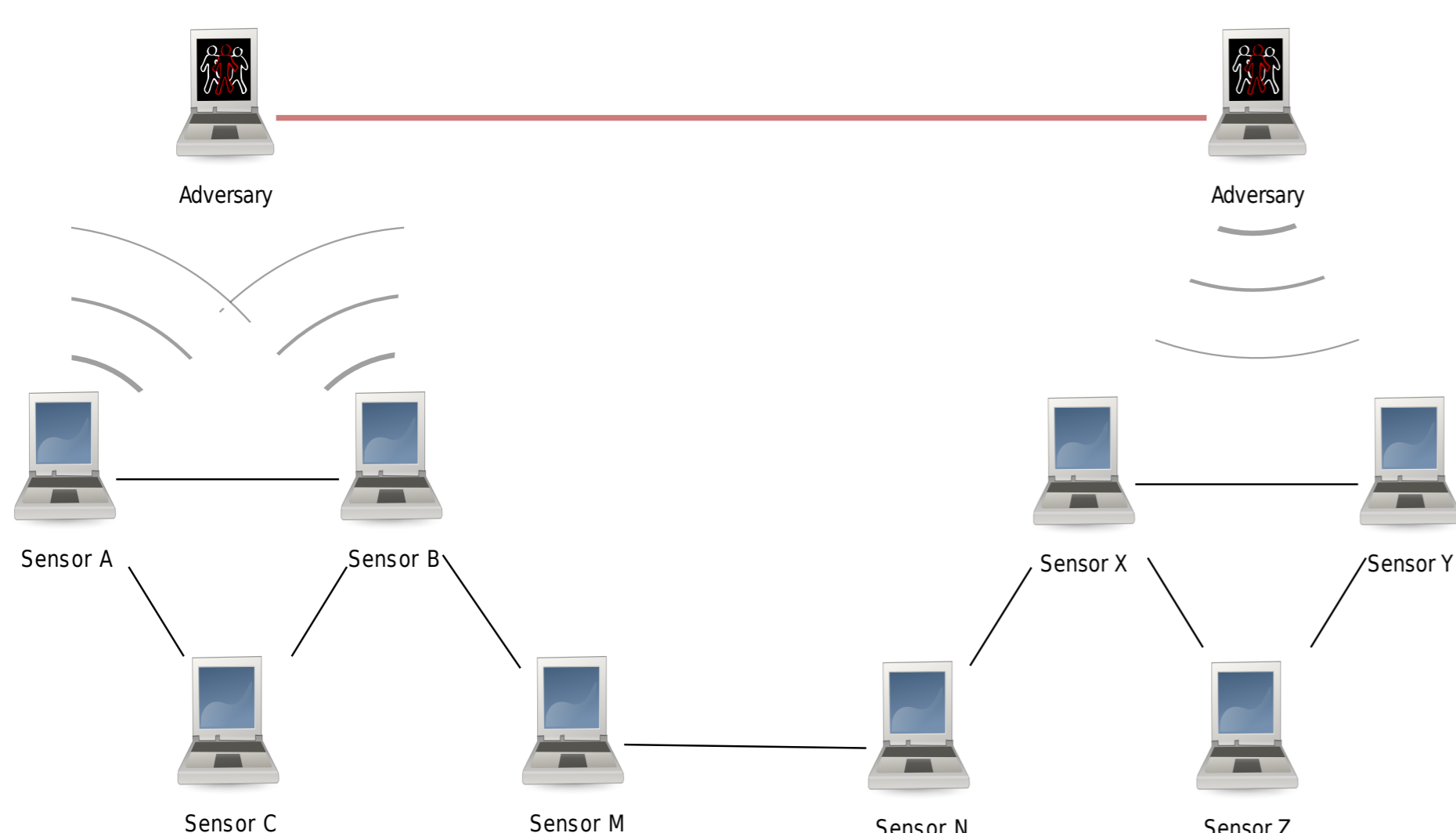


Figure 1: Wormhole attack in a multi-hop network

For a wormhole attack the adversary deploys several nodes within range of the sensor network. Messages received at one node are forwarded to the other and rebroadcast there. This means sensor events appear to occur at several places and the shortest routes are via the adversary-controlled wormhole. e.g. both A and B believe they are neighbours of X and Y. The shortest route between A/B/C and X/Y/Z is via the wormhole instead of via the M/N path.

POSITIVE ACKNOWLEDGMENT

Our intuition is that the positive acknowledgment used by wireless networks can be used to expose an impersonation attack. The adversary can disrupt communications between legitimate parties by deleting, delaying, re-ordering and modifying traffic. The ACK however, is special in that an attacker *must* take special measures to ensure that an ACK received by the sender within the ACKtimeout. Otherwise the sender becomes aware of a problem and will attempt to retransmit before signalling an error to the upper layers. When the minimum time taken to relay a frame is longer than the ACKTimeout an adversary can be exposed. Figure 2 shows an 802.11b timing diagram which shows why an adversary cannot simply relay the ACK.

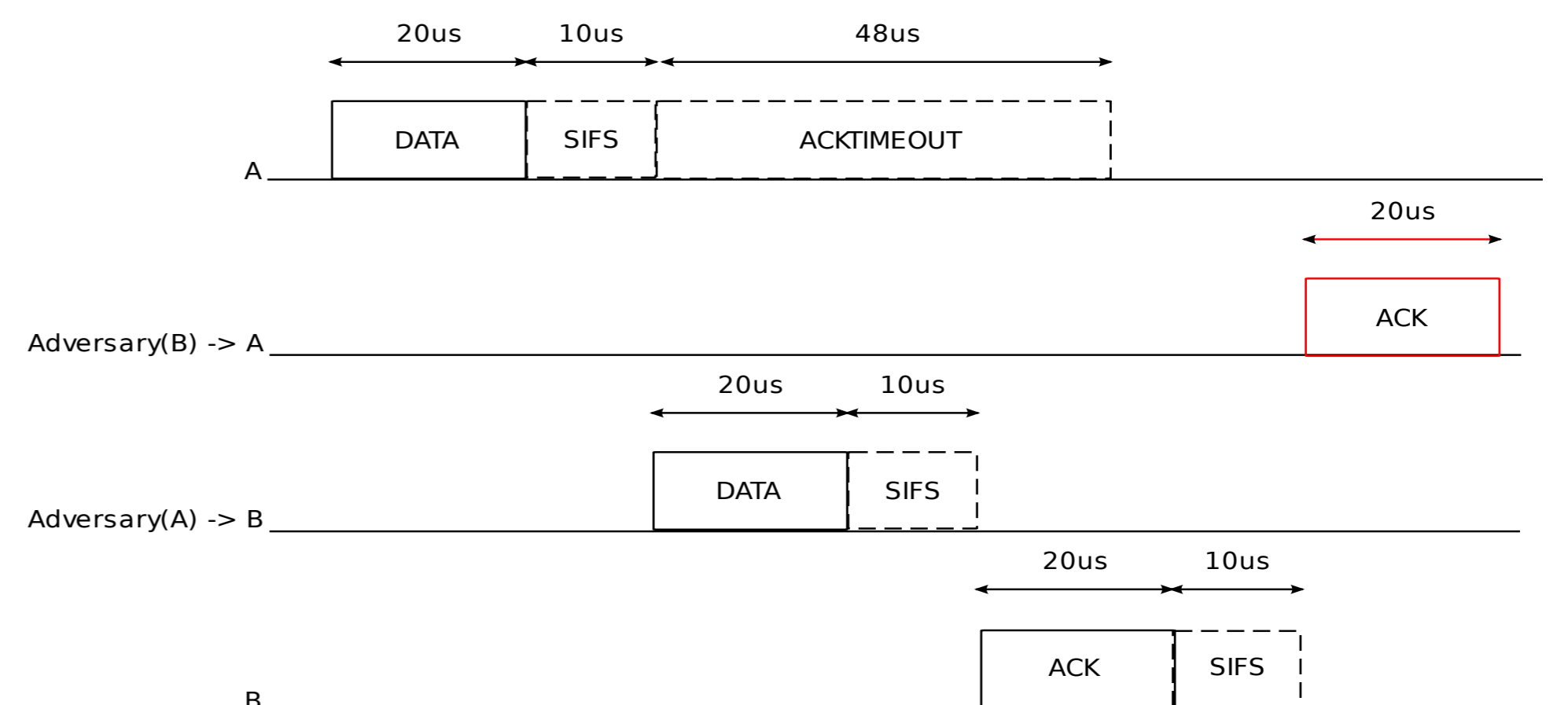


Figure 2: 802.11b timing diagram showing ACK relaying exceeds ACKTimeout

DETECTION

To detect an impersonator we have investigated a simple change to the MAC layer protocol which is being tested using 802.11 equipment. In this case a small percentage of frames are not acknowledged until the *n*th transmission but which frames these are and what the value of *n* requires knowledge of the session key.

```

SEND-DATA(packet )
1 n ← 0
2 ack ← NIL
3 while ack = NIL and n < maxtries
4   do n ← n + 1
5     SET-TRANSMIT-COUNT( packet , n)
6     TRANSMIT( packet )
7   ack ← RECV-ACK(ACKTIMEOUT)
8 if ack = NIL and n ≤ THRESHOLD( packet )
9   then error ACK is not authentic

RECV-DATA(packet )
1 n ← GET-TRANSMIT-COUNT( packet )
2 if n ≤ THRESHOLD( packet )
3   then No acknowledgment
4   else TRANSMIT(ACK)
5 ...
    
```

Figure 3: MAC protocol modifications for impersonator detection

PREVENTION

The preventative measure is to require the receiver to return a MIC for the plaintext of every received frame and send that MIC in the ACK. To prevent replay each packet will require a transmission count and a nonce - for sensors choosing the size of these fields will trade-off the risk of repla

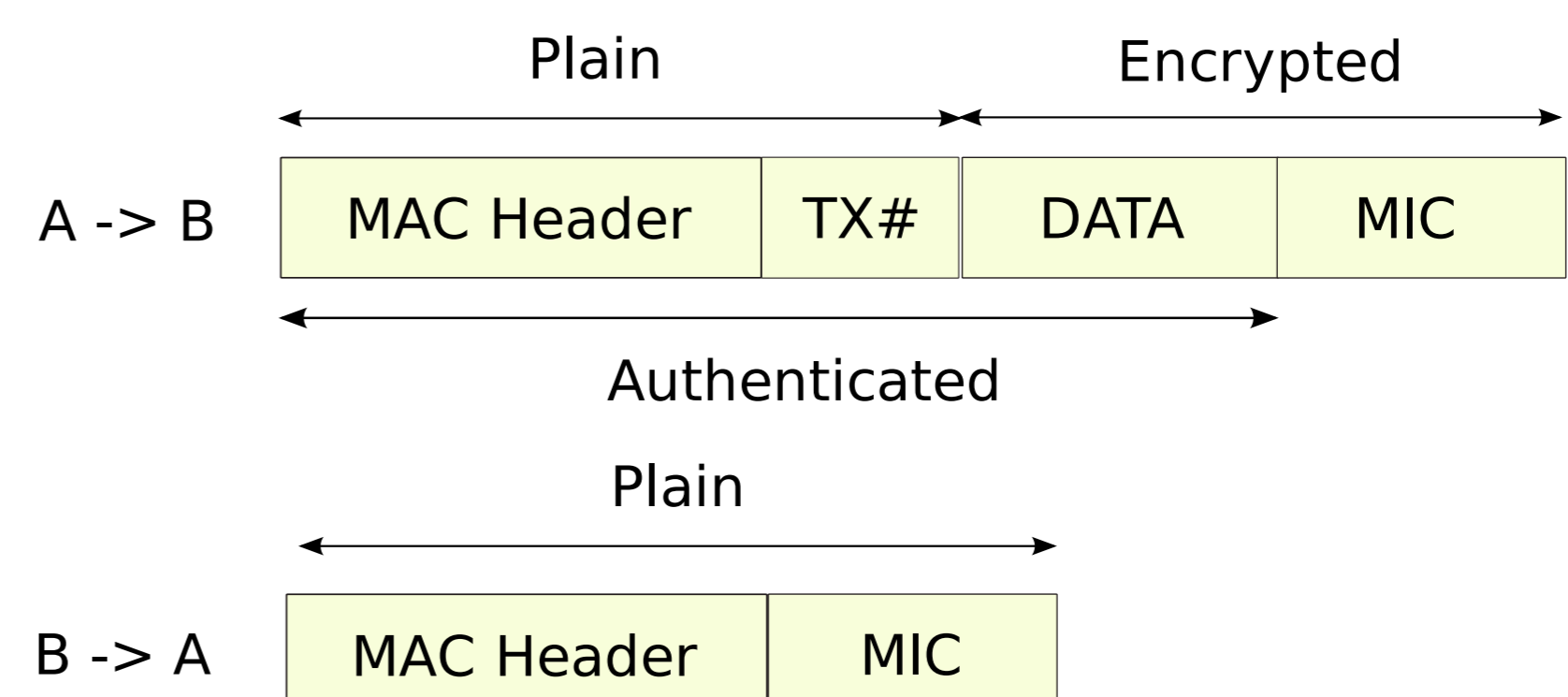


Figure 4: MAC frame modifications for impersonator prevention

REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370-380, February 2006.