Wireless patient monitoring systems: Can Black hole and Selective forwarding attacks be stopped?

In the past decades there have been advancements in technology and medical science. The two field are going hand-in-hand for providing better care to the people. For example, an automated patient monitoring system allows the vitals of a patient to be monitored while they are in their comfort zone. This has several advantages: 1) It frees the hospital staff from mundane tasks, 2) allows the doctors to get real-time information on a patient's vitals e.g. heart rate, blood pressure, and so on, and 3) The patients can move around freely without the need to be stuck in a bed.

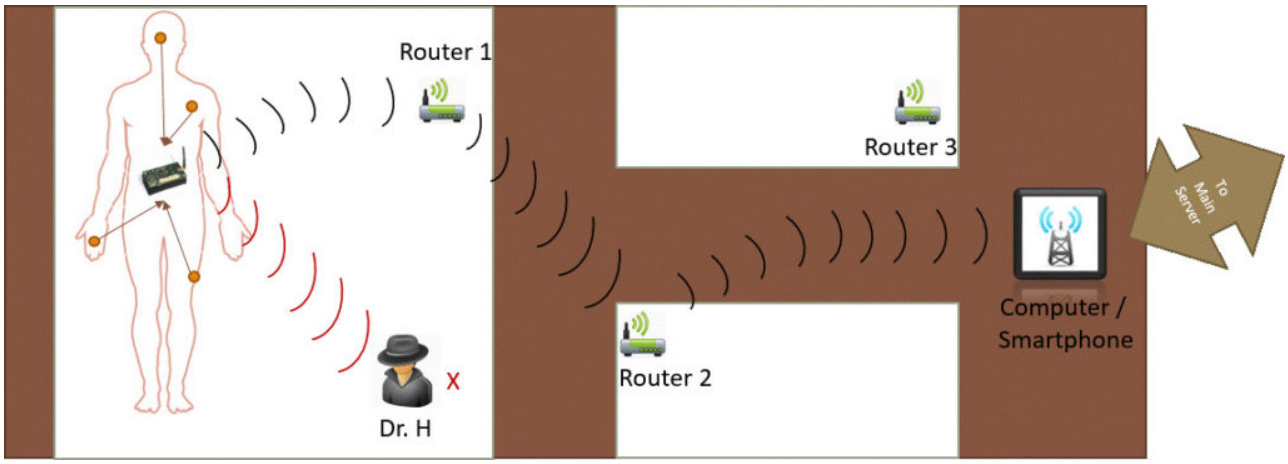

Fig. 1. Wireless patient monitoring system.

Figure 1 shows an automated patient monitoring system. Here the sensors are attached to a patient's body. These sensors gather the patient's vitals (heart rate, blood pressure etc.). Following this, they send this data to the nearest router (Router 1). Router 1 then forwards this data to other routers, which then forward it to the Base Station (BS). The BS may be a smartphone or may be connected to a computer. The BS then transmits this data to the hospital server from where it may be accessed by the hospital staff using their smartphones or computers.

This route (Sensors -> Router 1 -> Router 2 -> BS) is formed when the BS requests the sensors to send patient's vitals. The route is dynamic in nature, i.e. if the patient moves to another room the nearest router may be Router 2 or Router 3 thus changing the path i.e. (Sensors -> Router2 -> BS or Sensors -> Router 3 -> BS). So if an attacker, say Dr. H, sends a fake request packet during this route formation phase. Then the route may be compromised (Sensors -> Dr. H). Dr. H may or may not forward the data. If Dr. H does not forward any data packets then the attack is called Black-hole, else if Dr. H forwards some packets then the attack is called Selective-forwarding. These attacks are collectively known as denial of service attacks (DoS), which, as the name suggests,

denies service to a user.

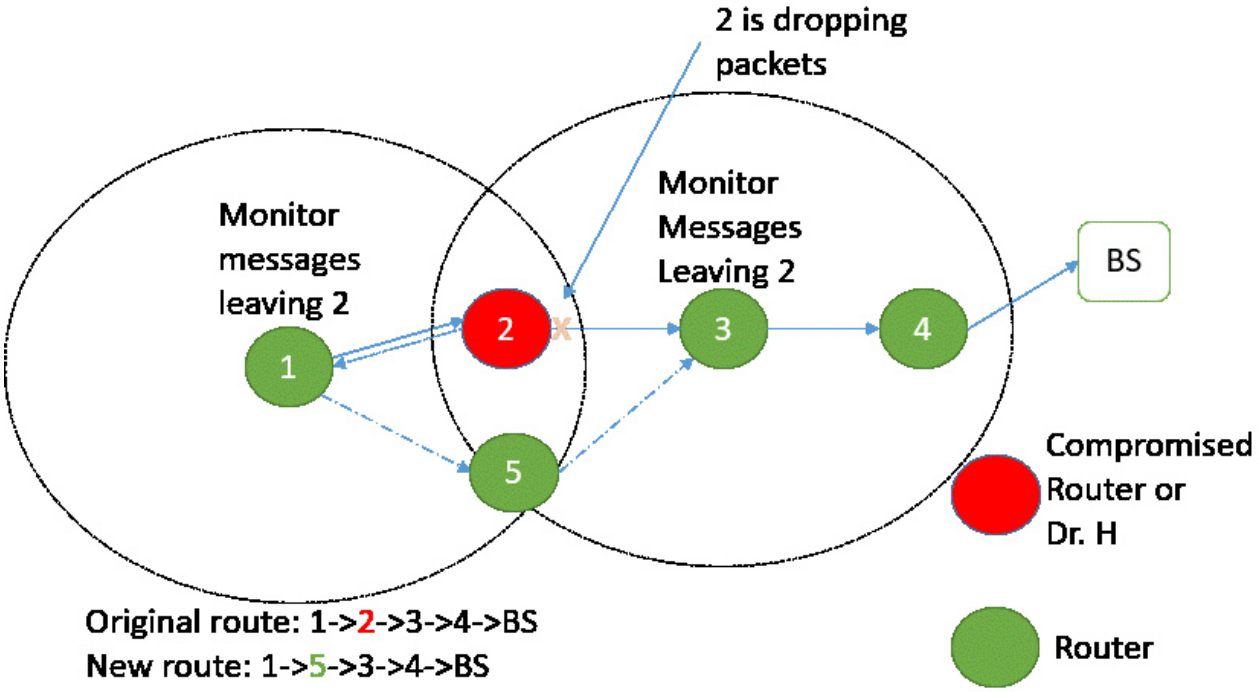

Fig. 2. Selective forwarding defence.

Since these DoS attacks can make the monitoring system useless, we devised a method to prevent and correct them. First, the initial agreement between the patient sensors and the BS (via. routers) is made forge-proof (i.e. Dr. H cannot pretend to be the BS). This is done by making use of random numbers and cryptographic hashes, which are complex one-way mathematical functions, making it impossible for Dr. H to reproduce the request send by the BS to the sensors. Thereby preventing the black-hole attack.

Second, consider that data travels from sensors to routers: 1 -> 2 -> 3 -> 4 and then to BS. Here the routers make use of neighbourhood-watch i.e. every router keeps track of messages leaving its neighbour, see Figure 2. Where, for example, router 1 and 3 are monitoring 2. This is coupled by analysis at the BS, which detects an imbalance in the number of packets flowing through the network and initiates selective forwarding detection. This detection allows the BS to know which routers are misbehaving. Thus, getting rid of router (2), and forming a new path: sensors -> 1 -> 5 -> 3 -> 4 -> BS.

In summary, our method secures a wireless patient monitoring system against Black-hole and Selective forwarding attacks. Thus increasing confidence in the implementation and usage of these

systems.

Avijit Mathur, Thomas Newe *and* ***Muzaffar Rao***
Department of Electronic and Communication,
University of Limerick
Limerick, Ireland

Publication

Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT.
Mathur A, Newe T, Rao M.
Sensors (Basel). 2016 Jan 19