Analysis of the applicability of Wireless Sensor Networks attacks to Body Area Networks

Mariana Segovia, Eduardo Grampín, Javier Baliosian *
Facultad de Ingeniería, Universidad de la República
Montevideo, Uruguay
{msegovia,grampin,javierba}@fing.edu.uy

ABSTRACT

A Body Area Network (BAN) is composed by several sensors that may be implanted or placed around the human body, usually deployed for health-care applications. The sensors monitor one or more vital signs and communicate through a wireless network, allowing the patient to lead a normal life. Innovative health-care applications may be deployed using BAN capabilities, and therefore, security issues in BAN shall be carefully considered, since they may have a great impact in the patient's health. Adversaries might create fake emergency warnings, prevent legitimate warnings from being reported, exhaust battery power, produce excessive tissue heating, among other attacks. While efforts have been carried out in the industry and academia to define security requirements in Wireless Sensor Networks (WSN), more work is needed regarding BAN. In this paper, we consider the differences between BAN and WSN, and examine a selection of known WSN attacks that may be used to damage BAN. We also present a stack based classification of these attacks, and we analyse the security impact of single-hop and dynamic multi-hop topologies in possible routing attacks. Finally, we review some security solutions and their cost in resources utilization.

Categories and Subject Descriptors

A.1 [**Introductory and Survey**]: Miscellaneous; C.2.0 [**Computer-Communication Networks**]: General—*Security and protection, wireless communication*

General Terms

Security

Keywords

Body Area Networks, Wireless Sensor Network, Security

1. INTRODUCTION

The development of clinical data knowledge has the potential to transform health-care since it provides better information to base care decision and scientific research. More detailed information allows physicians to provide a more accurate diagnosis and a better treatment. However, patients may refuse to divulge important information in cases of health problems, as their disclosure may lead to social stigma and discrimination.

*This work was partially funded by the Latin American and Caribbean Collaborative ICT Research Federation (LACCIR).

BODYNETS 2013, September 30-October 02, Boston, United States

DOI 10.4108/icst.bodynets.2013.253720

A BAN implements remote, continuous, digital and in real time physiological variables monitoring. Physiological variables are analog signals that correspond to human's physiological activities or body actions such us electrocardiograms, electromyograms, electroencephalograms, blood glucose, blood pulse, movements, temperature, and others. BANs have great potential to improve health-care; treatment of many diseases would benefit from real time monitoring, including hypertension, asthma, Alzheimer, Parkinson, diabetes, chronic bronchitis, renal failure, and prevention of sudden infant death syndrome.

Conventional security and privacy mechanisms are not suitable for BAN due to limitations in computational capabilities, memory, communication bandwidth, and battery power. In addition, an extremely low transmit power per node is needed to minimise interference, and account for health concerns.

The rest of this paper is organised as follows. Section 2 analyses the differences between BAN and WSN, while Section 3 provides a stack-based classification of WSN attacks that can be used against BAN. Finally, proposed solutions are presented in Section 4, and Section 5 draws some concluding remarks.

2. DIFFERENCES BETWEEN BAN AND WSN

Al-Saud et al. [1] define a Wireless Sensor Network (WSN) as 'an infrastructure-fewer network that consists of a number of self-configuring wireless devices capable of sensing vital signs for characterising contemporary phenomena. Such vital signs include, but not limited to, air quality, ambient temperature, pressure, human heart and brain signals'. The sensors read data and transmit it over a wireless communication channel to a base station that will be gathering raw data; typically, a running application analyses the collected data and takes decisions accordingly.

One of the WSN potential instances is a BAN for measuring physiological variables. The sensors can be located on the body as patches, integrated into clothes or even implanted into the body. The monitored signals are gathered by a personal device, such as a smart phone which acts as a sink for data of the sensor nodes and transmits them to health-care professional for health monitoring, data processing, analysis and storage [16].

Security and privacy issues are raised automatically when the data is created, transferred, stored and processed in information systems. Especially, data transfers for medical and health-care purposes should be secure, safe and reliable [6]. In view of the emerging threats, several important regulations have been enacted by governmental organisations in different countries. Conventional security and privacy mechanisms are not suitable for BAN due to limited computational capabilities, memory, communication bandwidth, and battery power. For this reason, it is challenging to implement the cryptographic algorithms and protocols required to meet the security requirements.

Devices communication in BAN borrow techniques from WSN. However, many WSN protocols and algorithms are not suitable for BAN particular features and requirements. Although the characteristics and constraints of WSNs may vary in each specific application, the main differences between WSN and BAN are showed in Table 1.

Table 1: Differences between BAN and WSN [16]

	BAN	WSN
Architecture	Three categories of nodes: sensors, actuators and relay nodes.	Every node operates as a sensor node as well as a router node.
Density	Redundancy is not required, and therefore BAN do not require high node density.	Fault tolerance is required, thus high node density is needed in WSN deployment.
Data Rate	Measured health signals generate near periodic information with an stable data rate.	WSN are usually used for event-based monitoring, where events can happen at irregular intervals.
Scale	Human body (cm/m)	Monitored environment (m/km)
Node Number	Fewer, limited in space (less than 20 nodes)	Many redundant nodes for wide area coverage (tens to hundreds of thousands of nodes)
Impact of data loss	May require additional measures to ensure quality of service and real-time data delivery	Likely to be compensated by redundant nodes.
Physical exposure	Since nodes are in a human body, attackers cannot easily gain physical access to the devices.	Deployed in a hostile environment, open to adversaries, bad weather, etc. The probability a sensor suffers a physical attack in such an environment is really high.

3. ATTACK CLASSIFICATION

BAN and WSN have many differences. However, many of the typical WSN attacks can be carried out against a BAN. In this section, we present a classification of such attacks based on the protocol stack.

3.1 Physical layer attacks

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption [18]. Some of the well-known attacks at this layer are:

1. **Jamming**: Jamming is the transmission of radio signals to interfere with the radio frequency being used by the sensor network. It can be produced intentionally or accidentally.

2. **Eavesdropping**: Eavesdropping is the interception and reading of messages by unintended receivers. WSN and BAN nodes share physical layer characteristics. Hence, jamming and eavesdropping may threaten BAN information.

Other attacks in this layer include i) *tampering*, which involves probing techniques that require access to the chip level components of the device to extract sensitive information such as cryptographic keys or other data on the node's memory chip, and ii) *side channel attack*, that refers to any attack that is based on the information gathered from the physical implementation of a cryptosystem. These attacks are relatively easy to perform in a WSN where nodes are generally in an outdoor environment and not physically protected. In BAN, they are hard to occur, since sensors may be implanted or located very close to the patient's body.

3.2 Data link layer attacks

The data link layer is responsible for multiplexing of data streams, data frame detection, medium access and error control [18]. Some of the well-known attacks at this layer follows.

1. **Collision**: A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When frames collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The frame will then be discarded as invalid [3].

2. **Exhaustion**: Some link layer protocols attempt retransmission repeatedly when a collision occurs. Hence, a malicious node may continuously disrupts the communication between two nodes, causing the source node to retransmit continuously. This leads to starvation of other nodes in the network with respect to channel access and exhausts the energy level of the nodes [3].

3. **Interrogation**: This kind of attack exploits the two-way Request To Send/Clear To Send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node's resources by repeatedly sending RTS messages to produce CTS responses from a targeted neighbor node [3].

These types of data link layer attacks may occur in BAN, since link layer protocols are similar in WSN and BAN.

3.3 Network layer attacks

A WSN is typically composed by hundreds or thousands of nodes organised in tree, cluster or mesh topologies. Every node behaves as a router receiving and forwarding data from other nodes. On the other hand, a BAN is usually organised in a star topology due to the small scale and short on-body link distance. The sensor nodes are not used to forward data or to exchange routing packets; they are directly connected to a coordinator node. For this reason, many of the common WSN routing attacks are not applicable in a BAN. However, the idea of cooperative communications for BAN is growing since researches have demonstrated that multi-hop architectures may be more effective than star architectures [2] [5] [6]. Braem et al. [2] compare the energy usage of multi-hop and single-hop transmissions in small-scale BAN experiencing high path loss, and show that in single-hop transmission, nodes far away from the sink perform much worse compared to the multi-hop case.
In addition to cooperative communications, the idea of using a dynamic network topology in BAN is also growing. The network topology may change due to factors such as human mobility, failures (link or power failure, etc.), addition of new nodes, great losses of RF signals, multi-path propagation that induce fading signals, among others.
Multi-hop architectures address the mobility of the human body using distributed relay nodes and dynamic routing protocols to find the best path for sensor nodes in each situation. In this manner, the attenuation of electromagnetic waves due to high path loss of the human body is also reduced. Another issue addressed by multi-hop architecture is to maintain low transmission power, in order to reduce the energy consumption and the SAR (Specific Absorption Rate) of radio signals. The absorbed radiation energy is converted to heat, and if too much heat is generated without being sufficiently regulated by the blood circulation system, the body tissue may be damaged. To prevent the bio-effect of radio signals on the human body high transmission power shall strictly controlled [5].
Single-hop and multi-hop topologies suffer different vulnerabilities and security considerations. A star topology has a single point of failure: the coordinator node; a successful attack directed to the coordinator may leave the entire network out-of-order. In a BAN of this type we do not need to take care of routing attacks such as selective forwarding, wormhole and sinkhole attacks. Hence, the security requirements are less complex than that of WSN. However, in a dynamic multi-hop topology the nodes are themselves routers. Thus packets are forwarded through different nodes before finding the destination. The possibility of node compromise or false nodes may create serious

vulnerabilities, especially routing attacks. In this case, several of the usual WSN attacks may be relevant to BAN, as follows:

1. **Spoofed, altered, or replayed routing information**: This type of attack may create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc [8]. In addition, an adversary can record messages and replay them, causing a waste of energy in the the receiver node [19].

2. **Blackhole**: In this attack a malicious node acts as a blackhole to attract all the traffic in the network [15]. For example, a malicious node may refuse to forward certain messages such as routing messages and simply drop them [19].

3. **Selective Forwarding attack**: The blackhole attack can be launched selectively. For example, dropping routing packets for a specific destination, a packet every t seconds, or a randomly selected portion of packets.

4. **Sinkhole attack**: In this attack an adversary tries to attract as much traffic as possible towards compromised nodes. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm [19].

5. **Wormhole attack**: In a wormhole attack the adversary records packets at one location in the network and tunnels them to another location [15]. This attack commonly involves two distant malicious nodes relaying packets along an out-of-bound channel available only to the attacker.

6. **Hello flood**: Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within a normal radio range of the sender. This assumption may be false because a laptop-class attacker with enough transmission power could convince every node in the network that he is its neighbor [8]. Then, they will route messages through the node sending the HELLO flood which most probably is not even within radio range [19].

7. **Acknowledgment spoofing**: In this attack, an adversary spoofs a bad link or a dead node using the link layer acknowledgment for the packets it overhears for those nodes [19]. Hence, it may convince the sender that a weak link is strong or that a dead or disabled node is alive.

8. **Node replication**: In a replication attack, the adversary first compromises a node, and then populates the network with replicas of it, using the secret key materials (node ID, secret cryptographic keys, etc.) extracted from the compromised node.

9. **Sybil attack**: The Sybil attack is defined as a malicious device illegitimately taking on multiple identities [13]. For example, a malicious node uses false identities or other legitimate nodes identities.

10. **Rushing attack**: A rushing attacker may exploit the multicast duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group [14]. If the route discovery packet forwarded by the attacker is the first to reach each neighbour node of the target, the neighbour will discard the subsequent packets transmitted by other nodes. To achieve this, the adversary quickly forwards route discovery packets by skipping processing or routing steps.

11. **Jelly Fish Attack**: This kind of attack delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real time data transmission [14].

3.4 Transport layer attacks

The security issues in transport layer are mainly due to flaws in the protocols. Hence, efficient design of the transport layer protocols can avoid transport layer threats. Well-known WSN attacks at this layer are:

1. **Flooding**: An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes [3].

2. **Desynchronisation**: This attack occurs when the adversary repeatedly forges messages to one or both end points which request transmission of missed segments. Hence, these segments are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information.

3.5 Application layer attacks

The vulnerabilities associated with this layer are mainly related with implementation of the applications. Thus, it is possible to exploit the problems caused by buffer overflow, memory leaks or parameters injection, among others.

1. **Software-based attack**: This type of attack is concerned with modifying the code, and exploiting known vulnerabilities. An example of this type of attack is the buffer overflow attack.

2. **Deluge/Reprogram attack**: Network programming system let you remotely reprogram nodes in deployed networks. If the reprogramming process is not secure, an intruder can hijack this process and take control of a network[3].

Another application layer WSN attack is the *overwhelm attack*, where an attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to the base station [3]. However, this WSN attack is hard to apply in BAN because is difficult to create false data without being noticed by the patient.

4. PROPOSED SOLUTIONS

In this section we provide an overview of current proposed security solutions in order to provide authentication, integrity and confidentiality. One of the main issues in BAN is energy consumption. For this reason, we focus on the energy cost of the proposed schemas.

Software Encryption

TinySec: TinySec is the first fully-implemented link layer security architecture for WSN. It addresses the WSN extreme resource constraints. It provides access control, message integrity, and message confidentiality [7]. However, it does not provide safeguards against resource consuming attacks, resistance to physical manipulation or capture node attack.
TinySec increases the computational and energy costs of sending information due to two main components [7]: larger packet sizes and extra computation time and energy needed for cryptography. Karlof et al. [7], using Mica2 motes, showed that the total energy consumed to send a 24 bytes packet was 3 % greater for the TinySec-Auth mode and 10 % greater for the TinySec-AE mode with respect to the "legacy" TinyOS stack.

Elliptic Curve Cryptography: Studies such as [10] have shown that it is possible to apply public key cryptography such as Elliptic Curve Cryptography (ECC) to BAN by using the right selection of associated parameters, optimisation and low power techniques [11].

Biometrics: Biometric information collected from the human body can uniquely represent an individual. In addition, it is hard to be deprived by suspicious intruders [17]. For these rea-

sons, it is used in proposed security systems for BAN. Mana et al. [12] present a security scheme that uses electrocardiogram signals to constitute symmetric cryptographic keys in BAN. They implement the AES algorithm with 128 bits key length; the total energy cost of their protocol is 28, $13mJ$ (including mutual authentication).

Hybrid security structure: Hybrid security structures (such as the one presented by Liu et al. [11]) combine symmetric and asymmetric algorithm for BAN. In general, asymmetric cryptographic algorithms are employed only in the association process due to the greater computation resources consumption. Once a trusted communication channel is established, symmetric cryptographic algorithms are used to provide security of exchanged data.

Hardware Encryption
Other option is to use hardware encryption instead of software encryption, such as the implemented in the ChipCon 2420 ZigBee compliant RF Transceiver. According to [4] hardware encryption does not significantly increase power consumption on the sensor motes. It is due to the efficient on-chip hardware support for encryption on the wireless controller and the dominant power consumption of the radio frequency unit when compared to the processing circuitry. Lee et al. [9] have measured the execution time and energy consumption of AES-128 on both MicaZ and TelosB for software and hardware AES encryption. Their experiments show an improvement grater than one order of magnitude in hardware implementations.

5. CONCLUSION AND FUTURE WORK

BAN can revolutionise health-care and improve quality of life due to the potential to offer a variety of benefits to patients and medical staff through continuous, remote and real-time monitoring as well as early detection of possible health problems. However, it brings out a new set of challenges in terms of security and privacy requirements, taking into account BAN resource constraints. In this study, we analyse those security requirements, using WSN well-known attacks as a base. We discuss which attacks may be used in BAN, providing a stack base classification of them. We conclude that the network topology has a great impact on routing security consideration. Security issues in a single-hop star topology are less complex than in a multi-hop routing topology, which, in turn, is more efficient. Hence, when designing a BAN the trade-off between efficiency and security shall be carefully considered; striking the right balance between these conflicting goals is very challenging.
To further explore BAN security requirements, we are carrying out both, functional and scalability tests. On the one hand, we are implementing a suite of link- and network-layer attacks in a BAN prototype comprised of TinyOS-based sensors and, on the other hand, we are using a WSN simulator for scalability purposes. We are also developing a proof-of-concept health-care application to have a glimpse of the applicability of security countermeasures in this environment.

6. ACKNOWLEDGMENTS

The authors would like to thank the team of the project "A Proposal for Security Management of Mobile Health and Medical Imaging" funded by LACCIR and the networking staff at UdelaR for their support.

7. REFERENCES

[1] K. A. Al-Saud. Wireless body area sensor networks signal processing and communication framework: Survey on sensing, communication technologies, delivery and feedback. *Journal of Computer Science*, 1(8):121–132, 2012.

[2] B. Braem, B. Latre, I. Moerman, C. Blondia, E. Reusens, W. Joseph, L. Martens, and P. Demeester. The need for cooperation and relaying in short-range high path loss sensor networks. In *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*, pages 566–571, 2007.

[3] H. Chaudhari. Wireless sensor networks: Security, attacks and challenges. *International Journal of Networking*, 1(1):04–16, 2011.

[4] G. Crosby, T. Ghosh, R. Murim, and C. Chin. Wireless body area networks for healthcare: A survey. *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, 3(3), June 2012.

[5] A. Ehyaie, M. Hashemi, and P. Khadivi. Using relay network to increase life time in wireless body area sensor networks. In *World of Wireless, Mobile and Multimedia Networks Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*, pages 1–6, 2009.

[6] Y. Ge, L. Liang, W. Ni, A. A. P. Wai, and G. Feng. A measurement study and implication for architecture design in wireless body area networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pages 799–804, 2012.

[7] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, SenSys '04, pages 162–175, New York, NY, USA, 2004. ACM.

[8] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pages 113–127, 2003.

[9] J. Lee, K. Kapitanova, and S. H. Son. The price of security in wireless sensor networks. *Comput. Netw.*, 54(17):2967–2978, Dec. 2010.

[10] A. Liu and P. Ning. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In *Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on*, pages 245–256, 2008.

[11] J. Liu and K.-S. Kwak. Hybrid security mechanisms for wireless body area networks. In *Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on*, pages 98–103, 2010.

[12] M. Mana, M. Feham, and B. A. Bensaber. Trust key management scheme for wireless body area networks. *I. J. Network Security*, 12(2):75–83, 2011.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, IPSN '04, pages 259–268, New York, NY, USA, 2004. ACM.

[14] V. Palanisamy and P. Annadurai. Impact of rushing attack on multicast in mobile ad hoc network. *CoRR*, abs/0909.1402, 2009.

[15] A. Pathan, H.-W. Lee, and C. seon Hong. Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 2, pages 6 pp.–1048, 2006.

[16] S. Ramli and R. Ahmad. Surveying the wireless body area network in the realm of wireless communication. In *Information Assurance and Security (IAS), 2011 7th International Conference on*, pages 58–61, 2011.

[17] S. Ramli, R. Ahmad, M. Abdollah, and E. Dutkiewicz. A biometric-based security for data authentication in wireless body area network (wban). In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pages 998–1001, 2013.

[18] J. Sen. A survey on wireless sensor network security. *International Journal of Communication Networks and Information Security (IJCNIS)*, abs/1011.1529(2), 2010.

[19] P. Stavroulakis and M. Stamp. Handbook of information and communication security. *Springer*, 2010.