Cryptanalysis of an Anonymous Mutual Authentication Protocol for Wireless Body Area Network

Azeddine Attir
Computer Science Department, LIAM Laboratory, University Mohamed Boudiaf of M'sila, M'sila, Algeria

Keywords: WBAN, Anonymous Authentication, Key Agreement.

Abstract: Wireless body area networks (WBANs) represent an important entity in E-health system, these networks offer enhanced efficiency, flexibility, and cost savings to patients, healthcare providers, and medical professionals in home- as well as hospital-based scenarios. The authentication of sensors is an essential security task. To the best of our knowledge, (Li et al, 2017) proposed the lightest authentication and key agreement scheme for WBAN. However, (M. Koya and Deepthi P. P, 2018) show that the Li et al. scheme is vulnerable to impersonation attack and they proposed to use the biokeys extracted from the inter pulse interval (IPI) to defend this attack. In this paper, we demonstrate that the M. Koya and Deepthi P. P scheme is vulnerable from sensor node spoofing attack hence, it does not provide anonymity. Subsequently we propose a security solution tackled with such vulnerability.

1 INTRODUCTION

A WBAN consists on a set of biosensors located in, on or around a human body and wirelessly communicate. The impact of wireless body area network (WBAN) in providing improved healthcare service is gaining active attention among the research community. WBAN systems are crucial in driving developments in the field of healthcare, as they provide the basis for information-based diagnosis and treatment of various diseases (M. Koya and Deepthi P. P, 2018). The star topology is the simplest and the widest used topology for WBAN, in which several sensors are scattered on different part of the human body and communicate directly with a central unit called hub (IEEE Std 802.15.6, 2012). However, nodes that are far away from the hub require higher energy for communication, and it could be harmful to the patient, especially when the nodes are attached or implanted inside the patient's body (Li et al, 2017). An extended architecture for WBAN has been adopted, in which a resource riche super node is introduced as a relay node between sensor nodes and the hub forming a two tiers WBAN architecture. Figure 1 shows a typical tow-tiers architecture of WBAN.

Sensor nodes collect vital signs such as electrocardiogram (ECG), electroencephalogram (EEG),photo-plethysmogram(PPG), electromyogram (EMG), blood pressure, and body temperature, and sends them to the super node which relays them to the hub. In response, the hub sends the appropriate commands to sensor nodes. Data must be communicated between the nodes and the hub in a secure manner. Anonymous mutual authentication and key agreement scheme is one of security solution used for WBAN. It consists of allowing sensor nodes attached to the patient's body to authenticate with the local hub node and establish a session key in an anonymous and unlinkable manner (Li et al, 2017).

Li et al. (Li et al, 2017) have proposed a lightweight authentication scheme for WBAN. The scheme uses temporal identity to provide anonymity and proposes a new security protocol to ensure authentication and session key creation. The proposed scheme protects against various existing attacks and it is energy efficient and presents lower computational cost than the other existing protocols.

M. Koya and Deepthi P. P (M. Koya and Deepthi P. P, 2018) have proposed a security enhancement of the Li et al (Li et al, 2017) scheme with a reduction in communication overhead between the sensor node and hub. In this paper, first we analyze the M. Koya and Deepthi P. P scheme and show that it is

Attir, A.
Cryptanalysis of an Anonymous Mutual Authentication Protocol for Wireless Body Area Network.
DOI: 10.5220/0010829000003118
In *Proceedings of the 11th International Conference on Sensor Networks (SENSORNETS 2022)*, pages 129-133
ISBN: 978-989-758-551-7; ISSN: 2184-4380

vulnerable to node spoofing attack. Second we propose a new security solution that protects the M. Koya and Deepthi P. P from the node spoofing attack hence, it provides anonymity.

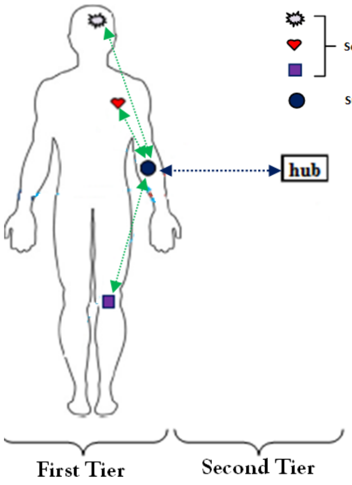


Figure 1: Architecture of typical tow-tiers WBAN.

The paper is structured as follows: section 2 presents related works, section 3 reviews the M. Koya and Deepthi P. P. scheme and shows how it is vulnerable from the sensor node spoofing attack, section 4 presents and analyzes our solution to the sensor node spoofing attack of the M. Koya and Deepthi P. P. scheme while section 5 concludes the paper.

2 RELATED WORK

WBSN is an important entity for Internet of Things (IoT), this type of wireless networks are able to sense physiological signs of person and exchange them with cloud servers or other data customers. The security and privacy of sensors and associated data is of great importance especially for critical application like E-health.

In 2012, The IEEE have proposed the 802.15.6 (IEEE Std 802.15.6, 2012), it purpose is to provide an international standard for a short-range (i.e., about human body range), low power, and highly reliable wireless communication for use in close proximity to, or inside, a human body. A number of security protocols are presented in the standard, however, rather than these security protocols are vulnerable to a wide range of attacks (M. Toorani, 2016), they are based on Elliptic Curve Cryptography (ECC) asymmetric cryptography which is not suitable for the wireless body area network with high energy limitation.

Anonymous and mutual authentication for WBAN is a hot research topic (Z. Zhao, 2014), (D. He and S. Zeadally, 2015), (D. He et al, 2016), (M.H. Ibrahim et al, 2016), (X. Li et al, 2017); all works in this area propose strong and lightweight solutions to be incorporated in IoT revolution. Cryptography based authentication schemes have been attracting increasing attention, recently, Li et al. (Li et al, 2017)presented an authenticated key agreement scheme suitable for WBANs, it is based only upon hash functions and exclusive or (XOR) operations, they do not require any additional infrastructure, and the associated computation and communication overheads are acceptable.

Khan et al. (H. Khan et al, 2018) have analyzed the Li et al. scheme (Li et al, 2017) and they find that it does not provide session unlinkability. In fact, they proposed a key agreement protocol that improves upon (Li et al, 2017) and provision requisite security and privacy properties, while preserving the efficiency offered by the original scheme.

M. Koya and Deepthi P. P (M. Koya and Deepthi P. P, 2018)have reviewed the Li et al. scheme and they find that is vulnerable to impersonation attack, in fact they proposed a new authentication solution over that scheme. In the next section, we review and analyze this new scheme and we show that is vulnerable to spoofing node attack.

3 SECURITY ANALYSIS OF THE M. KOYA AND DEEPTHI P. P SCHEME

3.1 Assumptions

M. Koya and Deepthi P. P gave the following assumptions in their paper:

– The adversary can eavesdrop, corrupt, replace, or replay the messages.

– The super node is assumed to be trustworthy.

– The threat model is the well-known Dolev-Yao model.

3.2 Review of the M. Koya and Deepthi P. P Scheme

The goal of the authentication scheme in (M. Koya and Deepthi P. P, 2018), is allows sensor nodes attached to the patient’s body to authenticate with the local hub node and establish a session key in an anonymous and unlinkable manner. This scheme includes two complimentary parts, the first one is the biokey part and the second is the cryptography part. In biokey part, sensor nodes and super node (Figure 1) extract biokeys -biokey represents parameter r_N in Figure 2, we notice that this parameter is generated with random number procedure in the Li et al. scheme (Li et al, 2017) - from the inter pulse interval (IPI) of cardiac recording, send them to the hub node, which computes the hamming distance between IPI of each sensor and super node, the hub pursues the authentication scheme -which is the second cryptography part of the scheme- only if this distance does not exceed a predefined threshold. In what follows, we review and analyze the cryptography part.

In the cryptography part, the system administrator (*SA*) is responsible for initialization and registration of sensor node N, super node *SN* and the hub *HN*. *SA* performs the following steps:

- Step 1: chooses a master secret key k_{HN} for *HN* and stores it in *HN's* memory.
- Step2: Picks a secret identity id_N (id_{SN}) for *N* (*SN*).
- Step 3: Picks k_N (k_{SN}) for *N* (*SN*).
- Step 4: Computes $a_N = id_N \oplus h(k_{HN}, k_N)$, $b_N = k_{HN} \oplus a_N \oplus k_N$, ($a_{SN} = id_{SN} \oplus h(k_{HN}, k_{SN})$, $b_{SN} = \; k_{HN} \oplus a_{SN} \oplus k_{SN}$).
- Step 5: Stores the tuple <id_N, a_N, b_N>in the sensor node's memory. (Stores the tuple <id_{SN}, a_{SN}, b_{SN}> in the super node's memory).

With $\oplus$ is bitwise XOR operation, *h()* the one way hash function, *(a, b)* the concatenation of data *a* and data *b*.

After the initialization and registration phase, sensor node and the hub start the authentication and key agreement phase. Figure 2 shows the authentication and key agreement scheme between *N* and *HN* with relay node *SN*.

3.3 Node Spoofing Attack

The major weakness of the scheme in (M. Koya and Deepthi P. P, 2018) is the ability of adversary to find the reel identity of the sensor node *N* which makes the scheme not anonymous. So, by intercepting communication between *N* and *HN*, the adversary is able to obtain the identity of node *N* only after the second session. Each session consist on the requesting authentication message sent from *N* to *HN* and responding message sent from *HN* to *N*. Figure 3 presents the steps performed by adversary

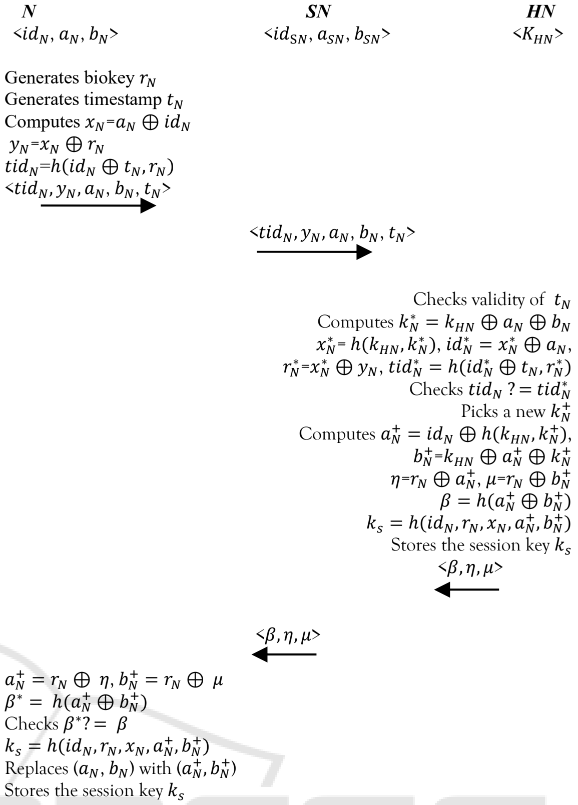

N
<id_N, a_N, b_N>
SN
<id_{SN}, a_{SN}, b_{SN}>
HN
<K_{HN}>
Generates biokey r_N
Generates timestamp t_N
Computes x_N=$a_N \oplus id_N$
y_N=$x_N \oplus r_N$
tid_N=$h(id_N \oplus t_N, r_N)$
<$tid_N, y_N, a_N, b_N, t_N$>
<$tid_N, y_N, a_N, b_N, t_N$>
Checks validity of t_N
Computes $k_N^* = k_{HN} \oplus a_N \oplus b_N$
x_N^*= $h(k_{HN}, k_N^*)$, $id_N^* = x_N^* \oplus a_N$,
r_N^*=$x_N^* \oplus y_N$, $tid_N^* = h(id_N^* \oplus t_N, r_N^*)$
Checks tid_N ?$= tid_N^*$
Picks a new k_N^+
Computes $a_N^+ = id_N \oplus h(k_{HN}, k_N^+)$,
b_N^+=$k_{HN} \oplus a_N^+ \oplus k_N^+$
η=$r_N \oplus a_N^+$, μ=$r_N \oplus b_N^+$
$\beta = h(a_N^+ \oplus b_N^+)$
$k_s = h(id_N, r_N, x_N, a_N^+, b_N^+)$
Stores the session key k_s
<β, η, μ>
<β, η, μ>
$a_N^+ = r_N \oplus \eta$, $b_N^+ = r_N \oplus \mu$
$\beta^* = h(a_N^+ \oplus b_N^+)$
Checks β^*?$= \beta$
$k_s = h(id_N, r_N, x_N, a_N^+, b_N^+)$
Replaces (a_N, b_N) with (a_N^+, b_N^+)
Stores the session key k_s

Figure 2: Cryptography part of M. Koya and Deepthi P. P scheme.

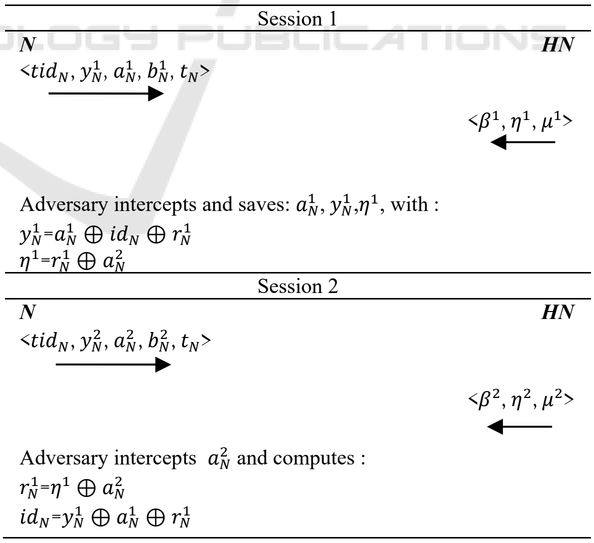

Session 1
N
HN
<$tid_N, y_N^1, a_N^1, b_N^1, t_N$>
<β^1, η^1, μ^1>
Adversary intercepts and saves: a_N^1, y_N^1,η^1, with :
y_N^1=$a_N^1 \oplus id_N \oplus r_N^1$
η^1=$r_N^1 \oplus a_N^2$
Session 2
N
HN
<$tid_N, y_N^2, a_N^2, b_N^2, t_N$>
<β^2, η^2, μ^2>
Adversary intercepts a_N^2 and computes :
r_N^1=$\eta^1 \oplus a_N^2$
id_N=$y_N^1 \oplus a_N^1 \oplus r_N^1$

Figure 3: Node spoofing attack in M. Koya and Deepthi P. P scheme.

to steal the node identity *id*$_N$, the exponent *i* of each parameter represents the actual session; for example: a_N^1 represents the parameter a_N used in the first session.

4 SECURING M. KOYA AND DEEPTHI P. P SCHEME FROM NODE SPOOFING ATTACK

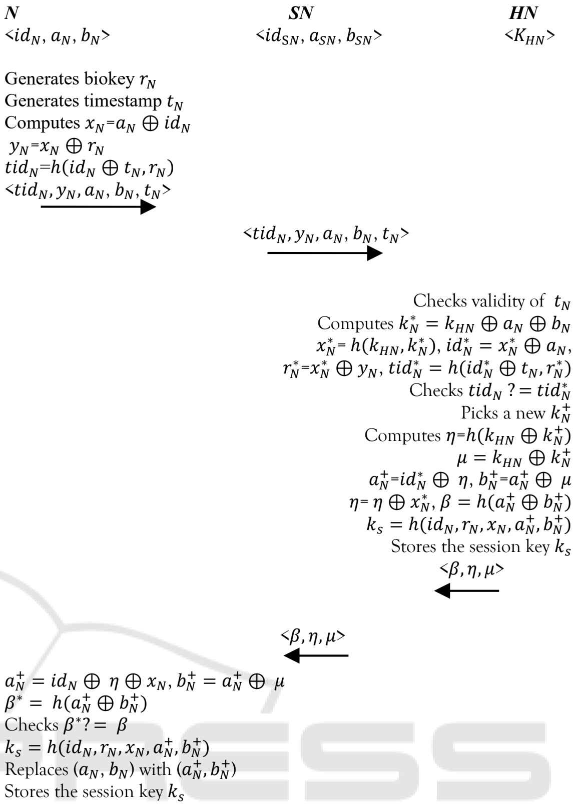
In this section we present our solution followed by a security analysis. From the session 2 in Figure 3, the adversary has obtained the identity *id*$_N$ of node *N* since it can computes the parameter *r*$_N$. Hence, we propose a method to prevent the adversary to obtain this parameter. So, we modify the scheme in Figure 2 in such a way we preserve the security of the scheme and prevent the adversary from computing *r*$_N$. The modification is done at *HN* and begin once *HN* authenticates *N*, i.e $tid_N == tid_N^*$. *HN* picks a new k_N^+ like in the original scheme, it computes: $\eta = h(k_{HN}, k_N^+)$ and $\mu = k_{HN} \oplus k_N^+$. Then *HN* computes: $a_N^+ = id_N^* \oplus \eta$, $b_N^+ = a_N^+ \oplus \mu$ and $\eta = \eta \oplus x_N^*$ .Next, *HN* pursuits the same operations of the original scheme. When *N* receives the message $< \beta, \eta, \mu >$, it computes: $a_N^+ = id_N \oplus \eta \oplus x_N$ and $b_N^+ = a_N^+ \oplus \mu$, and follows the sequence of operations of the original scheme. Figure 4 shows the improved scheme.

So, the new quantities add in our solution are the values of η and μ. Next we concentrate our security analysis only for theses quantities and we show how they protect the M. Koya and Deepthi P. P scheme from the node spoofing attack without affecting the security of the original scheme. Parameters likes tid_N, the timestamp t_N and β are not considered as there is no impact of our modification on that parameters.

From the scheme description in Figure 3, we know that x_N is the same as x_N^* of course when *HN* authenticates *N*. We name the quantity $h(k_{HN}, k_N^+)$: x_N^+ and we analyze the proposed solution in Figure 4 for two sessions.

In the first session, adversary intercepts the communication between *N* and *HN* and obtains the following quantities$y_N = x_N^* \oplus r_N$, *a*$_N$ and *b*$_N$. For the communication from *HN* to *N*, adversary obtains: $\eta = x_N^+ \oplus x_N^*$ and $\mu = k_{HN} \oplus k_N^+$.

So, the adversary obtains $\mu = k_{HN} \oplus k_N^+$ from our scheme as the same as in the original scheme by xoring a_N with b_N of the next session since, both parameters are sent in clear from *N* to *HN*. Also from Figure 3, μ does not contribute in the identity spoofing attack hence, there is no impact on the security of the original scheme.



N
<id_N, a_N, b_N>
SN
<id_{SN}, a_{SN}, b_{SN}>
HN
<K_{HN}>
Generates biokey r_N
Generates timestamp t_N
Computes x_N=$a_N \oplus id_N$
y_N=$x_N \oplus r_N$
tid_N=$h(id_N \oplus t_N, r_N)$
<$tid_N, y_N, a_N, b_N, t_N$>
<$tid_N, y_N, a_N, b_N, t_N$>
Checks validity of t_N
Computes $k_N^* = k_{HN} \oplus a_N \oplus b_N$
x_N^*= $h(k_{HN}, k_N^*)$, $id_N^* = x_N^* \oplus a_N$,
r_N^*=$x_N^* \oplus y_N$, $tid_N^* = h(id_N^* \oplus t_N, r_N^*)$
Checks $tid_N \,?= tid_N^*$
Picks a new k_N^+
Computes η=$h(k_{HN} \oplus k_N^+)$
$\mu = k_{HN} \oplus k_N^+$
a_N^+=$id_N^* \oplus \eta$, b_N^+=$a_N^+ \oplus \mu$
η= $\eta \oplus x_N^*$, $\beta = h(a_N^+ \oplus b_N^+)$
$k_s = h(id_N, r_N, x_N, a_N^+, b_N^+)$
Stores the session key k_s
<β, η, μ>
<β, η, μ>
$a_N^+ = id_N \oplus \eta \oplus x_N$, $b_N^+ = a_N^+ \oplus \mu$
$\beta^* = h(a_N^+ \oplus b_N^+)$
Checks $\beta^* ?= \beta$
$k_s = h(id_N, r_N, x_N, a_N^+, b_N^+)$
Replaces (a_N, b_N) with (a_N^+, b_N^+)
Stores the session key k_s

Figure 4: The improved scheme.

To following quantities resume what the adversary can obtain from the first session.

$$y_N = x_N^* \oplus r_N$$

$$a_N = id_N \oplus x_N^*$$

$$b_N = a_N \oplus k_{HN} \oplus k_N$$

$$\eta = x_N^+ \oplus x_N^*$$

$$\mu = k_{HN} \oplus k_N^+$$

We observe that all security parameters are protected with XOR operation, also when adversary tries to xor η with the other parameters it must fails to isolate any parameter. The adversary can do the following computations: $y_N \oplus \eta = x_N^+ \oplus r_N$, $a_N \oplus \eta = id_N \oplus x_N^+$,$y_N \oplus \eta \oplus a_N = id_N \oplus r_N$.

In the second session, adversary obtains:$y_N = x_N^+ \oplus r_{Nnew}$, a_N^+, b_N^+, $\eta = x_{Nnew}^+ \oplus x_N^+$, $\mu = k_{HN} \oplus k_{Nnew}^+$. The sign *new* is about all new parameters picked for the second session.

For the quantity $\mu = k_{HN} \oplus k_{Nnew}^+$ the result of security analysis is the same like in the first session.

The following quantities resume what the adversary can obtain from this session.

$y_N = x_N^+ \oplus r_{Nnew}$

$a_N = id_N \oplus x_N^+$

$b_N = a_N \oplus k_{HN} \oplus k_N^+$

$\eta = x_{Nnew}^+ \oplus x_N^+$

$\mu = k_{HN} \oplus k_{Nnew}^+$

Like in the first session, all security parameters are protected with XOR operation, also when adversary tries to xor η with the other parameters it must fails to isolate any parameter. If the adversary combines the parameters of both sessions, he can't isolate any parameter so, the xor of η of both sessions equals: $x_{Nnew}^+ \oplus x_N^*$ hence, there is no way for adversary to reach neither x_{Nnew}^+ nor x_N^*.

From the above analysis, our modification preserves the security of the M. Koya and Deepthi P. P scheme and prevents adversary to get the identity $id_N$of sensor node.

5 CONCLUSION

Anonymous mutual authentication and key agreement scheme is a key issue in wireless body sensor network, all researches in this area propose a strong and lightweight solutions. This paper analyzes the M. Koya and Deepthi P. P scheme and shows that it is venerable to sensor node spoofing attack. In fact, we have proposed a security countermeasure. In the future, we will continue to explore and resolve the security problems in WBAN.

REFERENCES

Li, X.; Ibrahim, M.H.; Kumari, S.; Sangaiah, A.K.; Gupta, V.; Choo, K.K.R. (2017),Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput. Netw, 129, 429–443.

Aneesh M. Koya, Deepthi P. P (2018), Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network, Comput. Netw. 140 138–151.

IEEE Std 802.15.6 (2012), IEEE standard for local and metropolitan area networks - part 15.6: Wireless body area networks. pp. 1–271, Feb 2012.

M. Toorani (2016), "Security Analysis of the IEEE 802.15.6 Standard," International Journal of Communication Systems, Vol.29, No.17, pp.2471-2489.

Z. Zhao (2014), "An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem", J. Medical Systems, vol. 38, no. 2, pp. 1-7.

D. He , S. Zeadally (2015), Authentication protocol for an ambient assisted living system, IEEE Commun. Mag. 53 71–77 .

D. He; S. Zeadally; N. Kumar; J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," in IEEE Systems Journal , 2016, pp.1-12.

M.H. Ibrahim , S. Kumari , A.K. Das , M. Wazid , V. Odelu (2016), Secure anonymous mutual authentication for star two-tier wireless body area networks, Comput. Methods Programs Biomed. 135 37–50 .

X. Li , M.H. Ibrahim , S. Kumari , R. Kumar (2017), Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors, Telecommun. Syst. 67 (2) 323–348.

H. Khan, B. Dowling, K. M. Martin (2018), Highly Efficient Privacy-Preserving Key Agreement for Wireless Body Area Networks, TrustCom.