Schéma Optimal basé sur la Preuve à Divulgation Nulle de Connaissance pour les Réseaux Wireless Body Area Networks (WBAN)

Gewu Bu, Maria Potop-Butucaru

To cite this version:

Gewu Bu, Maria Potop-Butucaru. Schéma Optimal basé sur la Preuve à Divulgation Nulle de Connaissance pour les Réseaux Wireless Body Area Networks (WBAN). ALGOTEL 2018 - 20èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, May 2018, Roscoff, France. hal-01781845v3

HAL Id: hal-01781845
https://hal.archives-ouvertes.fr/hal-01781845v3

Submitted on 30 May 2018

Schéma Optimal basé sur la Preuve à Divulgation Nulle de Connaissance pour les Réseaux Wireless Body Area Networks (WBAN)[†‡]

Gewu BU[1] et Maria POTOP-BUTUCARU[1]

[1] *Sorbonne Université, UPMC, LIP6, CNRS UMR 7606*

Nous proposons BAN-GZKP qui optimize BANZKP (un schéma à divulgation nulle de connaissances spécifiquement adapté aux réseaux corporels (Wireless Body Area Networks). BANZKP est vulnérable à certaines attaques de sécurité telles que l'attaque par rejeu, l'attaque par déni de services distribués (DDoS) et l'attaque par l'interception des informations redondantes. Etant donné que BANZKP demande une authentification de bout en bout, ce schéma n'est pas compatible avec la mobilité posturale du corps humain. Notre proposition, BAN-GZKP, améliore la sécurité et la tolérance à la mobilité posturale de BANZKP. Afin de corriger les vulnérabilités de BANZKP, BAN-GZKP utilise un mécanisme d'attribution de clés de cryptage aléatoires, sans coût supplémentaire en termes de mémoire, de complexité ou de consommation énergétique. En utilisant une authentification saut par saut, notre schéma BAN-GZKP devient tolérant à la mobilité posturale. Nous démontrons, par des simulations intensives, que BAN-GZKP améliore BANZKP en termes du taux de réception au niveau du sink (34.06%), du délai de bout en bout (36.02%) et du nombre de transmissions (14.11%) lorsque ce schéma est couplé à un protocole de convergecast. De plus, nous optimisons le schéma d'authentification du protocole originale qui nécessite cinq phases à un schéma utilisant uniquement trois phases tout en garantissant le même niveau de sécurité. Notre schéma devient donc optimal en nombre de phases.

Mots-clefs : Wireless Body Area Network (WBAN), Sécurité mobile et sans fil, Analyse de la performance du réseau, Preuve à Divulgation Nulle de Connaissance

---

1 Introduction

Wireless Body Area Networks (WBAN) is a kind of Wireless Sensors Networks (WSN). In WBAN, on-body sensors collect user's physiological Data and transmit them to a sink node. Sensors move with the human postural mobility, the network topology in WBAN therefore dynamically changes following the postural body mobility. Multi-hop WBAN communication proposed in [NWK$^+$15] easily adapts to postural mobility. Also, multi-hop communications need lower transmission power compared to one-hop direct communication. WBAN is sensitive to security and privacy attacks : any medical Data error, leakage or imitation may lead to a wrong medical treatment, which is life or death. The challenges of WBAN security is that the computing and storage capacity is limited to achieve complex security protocol. Also, dynamic lossy connections in WBAN hinder the messages exchanging of security protocol. The best to date, the Zero Knowledge Proof-based scheme, BANZKP [CPBK16], is proposed, who uses less memory and computing capacity than TinyZKP [MGZ14] and the Elliptic Curve Encryption Based Public Key Authentication [WSTL11]. BANZKP is resilient to a wide range of attacks.

However, BANZKP still suffers from some specific malicious attacks. Moreover, the resilience of BANZKP to human body postural mobility in WBAN environment is still an open question. We propose BAN-GZKP, to fix vulnerabilities of BANZKP. Based on an extensive analysis and simulations, we show BAN-GZKP outperforms BANZKP in terms of security and WBAN environment adaptation.

[†] An extended version of this paper has been published in IEEE MASS 2017

[‡] This research was supported in part by ANR ESTATE

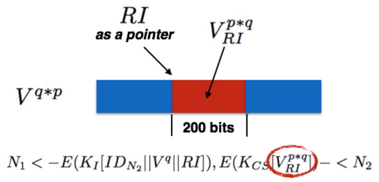

FIGURE 1: Representation of V_{RI}^{q*p}

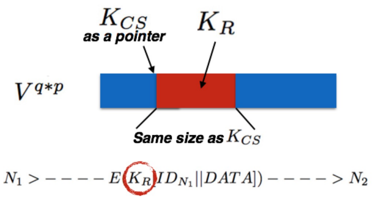

FIGURE 2: Representation of K_R

2 BANZKP Analysis

The idea of BANZKP end-to-end authentication [CPBK16] is to make two authentication entities (source and the destination) agree with each other that they hold the same secret number. This number V and a shared key K_I are set manually by user at the beginning for all the legal nodes. When a node N_1 wants to send Data to N_2, an authentication session is initiated as following :

$$\begin{aligned}
1)N_1 &> - - - - - -E(K_I[ID_{N_1}||V^p]) - - - - - - > N_2\\
2)N_1 &< -E(K_I[ID_{N_2}||V^q||RI]), E(K_{CS}[V_{RI}^{p*q}]) - < N_2\\
3)N_1 &> - - - - -E(K_I[ID_{N_1}||V_{RI}^{q*p}]) - - - - - - > N_2\\
4)N_1 &< - - - - - - - - K_{CS} - - - - - - - - - - < N_2\\
5)N_1 &> - - - - -E(K_I[ID_{N_1}||Data]) - - - - - > N_2
\end{aligned}$$

where ID_{N_1} and ID_{N_2} are identities of N_1 and N_2 respectively ; V is the secret number needing to be authenticated by N_1 and N_2 ; p and q are two random values generated by N_1 and N_2, respectively ; K_I is a shared key between N_1 and N_2 ; K_{CS} is a random key generated by N_2 and the function $E(K[a])$ means encrypt a with key K. RI is the indicator of the beginning of an interval value of V^{q*p}, represented by V_{RI}^{q*p}. In BANZKP, the size of this interval is 200 bits (see Figure 1).

The main authentications mechanisms of BANZKP are that from the computations of among V and random q and p, and the messages exchanging, both N_1 and N_2 can get V^{q*p} without sending the secret number V to the network. Notice that instead of sending of the whole V^{q*p}, in BANZKP, nodes only chose a part of V^{q*p} of 200 bits, V_{RI}^{q*p} and a pointer, RI. From receiving the message 3), N_2 can verify if the V_{RI}^{p*q} from N_1 is the same then which it holds. If yes, N_2 authenticated N_1 and send the K_{CS} to N_1 to decrypt V_{RI}^{p*q} sent in message 2). Then N_1 can verify if N_2 is legal node. By this way N_1 and N_2 can authenticate to each other. For the detailed descriptions of the authentication, please see [CPBK16].

BANZKP copes with the following attacks : **Forge Nodes**, **Replay Attack**, **Man in the Middle Attack**, **Guessing Attack** and **Privacy Attack** [CPBK16]. However BANZKP still suffers from same attacks : A constant K_I leads to the **Data Replay Attack** and **Redundancy Information Crack** and end-to-end authentication scheme leads to the **DDoS Attack at Sink**, please see [BPB18] for details of attack scenarios and defect analysis.

3 BAN-GZKP

In order to tolerate Data Replay Attack, Redundancy Information Crack and DDoS attack at sink BAN-GZKP uses two ingredients : **Random Key Allocation** and **Hop-by-Hop authentication scheme**. Conceding the high dynamic and unstable WBAN connections, we further propose **exchanging Scheme Optimization** to reduce the number of the exchanging for each authentications session.

Random Key Allocation Data Replay Attack and Redundancy Information Crack are possible in BANZKP because a constant key K_I is used to encrypt all Data messages [BPB18]. We give an effective Random Key Allocation mechanism for BANZKP.

The idea of the Random Key Allocation is as follows : when nodes authenticate, the value V^{q*p} will be obligatory computed for each authentication session. Since p and q are randomly chosen, V^{q*p} is also random. During the authentication message 4) in the original BANZKP, N_2 will send the random session key to N_1 to decrypt previous information. Notice that, even though K_{CS} is random, this key should not be used to encrypt Data messages because it has been sent on clear text. Our idea is to use K_{CS} as a random pointer that will point to a bit in the binary representation of the random value V^{q*p}. Then we chose an interval in the binary representation of V^{q*p} that starts with the bit pointed by the random pointer K_{CS}. This interval, of length K_{CS} can be seen as a random key, K_R, to encrypt Data message for the current session (see Figure 2). Our Random Key Allocation does not require additional keys at the initialization and does not need the transmission of additional fields in the exchanging message.

Hop-by-Hop Scheme Note that Sink-Side DDoS Attack happens in the end-to-end authentication scheme because relay nodes cannot detect whether the authentication message is legal or not, only the sink can do [BPB18]. To solve this problem and prevent Sink-Side DDoS Attack, we provide relay nodes with the capacity to detect invalid authentications.

The idea is as follows, instead of doing the authentication between the pair source-sink, we let source nodes to initiate authentication directly with their one-hop neighbours. After this authentication phase finishes with success, a source is allowed to send Data messages to the authenticated neighbour. The neighbour who receives Data messages can then initiate authentication with its neighbours until Data reaches to the sink. An adversary who wants to initiate a large number of invalid authentication requests to block the network will be detected directly by its one-hop neighbours and the DDoS Attack can thus be limited in a local range.

Exchanging Scheme Optimization When a source node N_1 initiates authentication with another node N_2 that previously authenticated with N_1 and that recognizes the identity of N_1, then N_2 instead of sending back $E(K_I[ID_{N_2}||V^q||RI]), E(K_{CS}[V_{RI}^{p*q}])$, where V_{RI}^{p*q} is encrypted with K_{CS} (as in original BANZKP scheme), it sends back directly V_{RI}^{p*q} encrypted with the initial key K_I. In our BAN-GZKP N_2 needs just to send a random pointer R for the Random Key Allocation. Hence, the final message sent back to N_1 is : $E(K_I[ID_{N_2}||V^q||RI||R||V_{RI}^{p*q}])$. After receiving the response of N_2, N_1 finishes the authentication using the same mechanism, and choses a random key, K_R, from the pointer R of Random Key Allocation and encrypt Data by K_R then sends the message to N_2. We thus can complete the authentication session after the first successful authentication between these two nodes. The scheme is as follows (we preserve the same notations as for the description of the BANZKP scheme) :

$$\begin{array}{l}
1)N_1 > ------E(K_I[ID_{N_1}||V^p])------ > N_2 \\
2)N_1 < --E(K_I[ID_{N_2}||V^q||RI||R||V_{RI}^{p*q}])-- < N_2 \\
3)N_1 > ----E(K_R[ID_{N_1}||DATA])---- > N_2
\end{array}$$

Even though BAN-GZKP reduces the number of authentication messages it tolerates the attacks tolerated by BANZKP scheme and also Data Replay Attack and Redundancy Information Crack. Please see [BPB18] for the proof details.

4 Performance Analysis

To compare the performance impact, we apply BANZKP and BAN-GZKP into five examples of five classes of convergecast strategies specified for WBAN from [BPB17] :**All Parents to All Parents Strategy** (APAP), **Tree-based Strategy**, **Collection Tree Protocol** (CTP), **FloodToSink Strategy** and **Attenuation-based Strategy** (MiniAtt). Convergecast means the sink node collect data packets sent from others source nodes.

We use the physical model proposed in [NWK$^+$15, BCPPB15]. This model issued from experiments with a network composed of seven sensors distributed on the body, six source nodes send Data, one sink node receives them. This model provide wireless channel attenuation information between each two nodes in seven different dynamic postures : 1) Walking, 2) Running 3) Walking weakly, 4) Sitting down, 5) Lying down, 6) Sleeping and 7) Wearing a jacket. In each posture, the model provide distributions of random wireless channel attenuation (on dB) between each two nodes. If the signal strength (on dBm) after passing the channel is smaller than the sensibility (on dBm) at the receiver, then the packet will be dropped. In this paper, we use the same simulation environment as in [BCPPB15] (IEEE 802.15.4) with a communication frequency of 2.45 GHz. The transmission power and the sensibility of the radio module of nodes are set

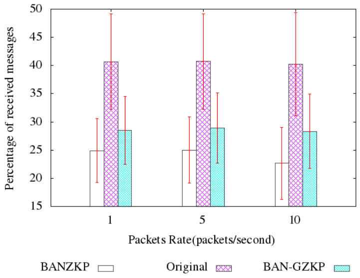

FIGURE 3: Reception Rates in Posture 1 Walking

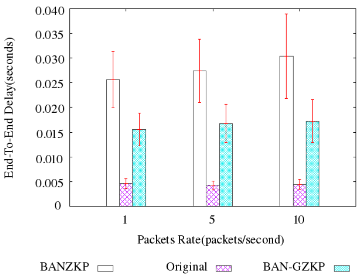

FIGURE 4: End-To-End Delay in Posture 1 Walking

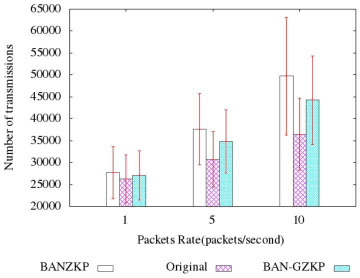

FIGURE 5: Total Number of Transmissions in Posture 1 Walking

to -60dBm and -100dBm respectively. We consider the following packet rates at the application layer : 1 packet/second, 5 packets/second and 10 packets/second, respectively.

Figure 3, 4 and 5 show the comparisons results of **ratios of Data packet reception at sink**, **end-to-end delay**, **number of transmissions** of CTP strategy in Posture 1 Walking. Due to the lack of space, please see [BPB18] for others simulations results. In each figure, the red columns represent the original CTP strategies without applying any authentication scheme ; the white columns represent original strategies applying BANZKP ; and the blue columns original strategies applying BAN-GZKP. When applying authentication scheme, WBAN performance decreases in general : lower ratio of packets reception, higher end-to-end delay and number of the transmissions, due to the additional ZKP authentication scheme added to the original one. When focusing on the comparison between BANZKP and BAN-GZKP, we noticed that BAN-GZKP has higher ratio of reception, lower end-to-end delay and number of transmissions. In conclusion, BAN-GZKP outperforms BANZKP by 34.06%, 36.02% and 14.11% in therms of ratios of Data packet reception at sink, end-to-end delay and number of transmissions, respectively.

Références

[BCPPB15] Wafa Badreddine, Claude Chaudet, Federico Petruzzi, and Maria Potop-Butucaru. Broadcast strategies in wireless body area networks. In *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 83–90. ACM, 2015.

[BPB17] Gewu Bu and Maria Potop-Butucaru. Total order reliable convergecast in wban. In *Proceedings of the 18th International Conference on Distributed Computing and Networking*, number 26. ACM, 2017.

[BPB18] Gewu Bu and Maria Potop-Butucaru. Ban-gzkp : Optimal zero knowledge proof based scheme for wireless body area networks. *Ad Hoc Networks*, 77 :28 – 41, 2018.

[CPBK16] Claude Chaudet, Maria Potop-Butucaru, and Nesrine Khernane. Banzkp : a secure authentication scheme using zero knowledge proof for wbans. In *The 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pages 1–7. IEEE, 2016.

[MGZ14] Limin Ma, Yu Ge, and Yuesheng Zhu. Tinyzkp : a lightweight authentication scheme based on zero-knowledge proof for wireless body area networks. *Springer Wireless personal communications*, 77 :1077–1090, July 2014.

[NWK$^+$15] Jun-ichi Naganawa, Karma Wangchuk, Minseok Kim, Takahiro Aoyagi, and Jun-ichi Takada. Simulation-based scenario-specific channel modeling for wban cooperative transmission schemes. *IEEE journal of biomedical and health informatics*, 19 :559–570, March 2015.

[WSTL11] Haodong Wang, Bo Sheng, Chiu C Tan, and Qun Li. Public-key based access control in sensornet. *Springer Wireless Networks*, 17 :1217–1234, July 2011.