Lightweight Encryption Based Security Package for Wireless Body Area Network

Sangwon Shin
South Dakota State University

Follow this and additional works at: https://openprairie.sdstate.edu/etd

Part of the Electrical and Computer Engineering Commons, and the OS and Networks Commons

Recommended Citation
https://openprairie.sdstate.edu/etd/5256

This Thesis - Open Access is brought to you for free and open access by Open PRAIRIE: Open Public Research Access Institutional Repository and Information Exchange. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Open PRAIRIE: Open Public Research Access Institutional Repository and Information Exchange. For more information, please contact michael.biondo@sdstate.edu.
LIGHTWEIGHT ENCRYPTION BASED SECURITY PACKAGE FOR

WIRELESS BODY AREA NETWORK

BY

SANGWON SHIN

A thesis submitted in partial fulfillment of the requirements for the

Master of Science

Major in Computer Science

South Dakota State University

2021
This thesis is approved as a creditable and independent investigation by a candidate for
the master’s degree and is acceptable for meeting the thesis requirements for this degree.
Acceptance of this does not imply that the conclusions reached by the candidate are
necessarily the conclusions of the major department.
ACKNOWLEDGEMENTS

I sincerely thank Dr. Sung, Shin for giving me excellent advice and opportunities on research in the field of computer science. I would also like to thank Dr. Kwanghee Won for advising my research with his knowledge; without him my thesis could not reach in current quality with chosen topic.

I appreciate professional feedback from all of my committee members: Dr Sung Shin, Dr Kwanhee Won. With provided feedback, my thesis quality has been improved.

I would also like to take this opportunity to thank my friends and colleagues in CCT lab who read the numerous drafts and helped me improve this paper; I can show my gratitude to my parents for their support thanks to their precious time spent for my research.
CONTENTS

ABBREVIATIONS...........................................................................................................v

LIST OF TABLES...........................................................................................................vi

LIST OF FIGURES..........................................................................................................vii

LIST OF EQUATIONS.....................................................................................................viii

ABSTRACT.........................................................................................................................ix

I. INTRODUCTION...........................................................................................................1

II. BACKGROUND.............................................................................................................3

2.1 WIRELESS BODY AREA NETWORK...........................................................................3

2.2 SECURITY THREATS.................................................................................................6

2.3 DATA AUTHENTICATION AND ENCRYPTION.......................................................7

2.4 SECURITY PROTOCOL.............................................................................................10

III. RELATED WORK.......................................................................................................11

IV. METHODS................................................................................................................13

4.1 PREPROCESSED SYMMETRIC RSA........................................................................14

4.2 RE-KEYING PROTOCOL..........................................................................................17

V. RESULTS AND EVALUATION......................................................................................20

VI. CONCLUSION............................................................................................................25

VII. LITERATURE CITED...................................................................................................26
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic-Curve Cryptography</td>
</tr>
<tr>
<td>E-MAC</td>
<td>Encryption based Message Authentication Code</td>
</tr>
<tr>
<td>GNFS</td>
<td>General Number Field Sieve</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MITM</td>
<td>Man In The Middle</td>
</tr>
<tr>
<td>PSRSA</td>
<td>Pre-processed Symmetric Rivet-Shamir-Adleman</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>WBAN</td>
<td>Wireless Body Area Network</td>
</tr>
<tr>
<td>ZKP</td>
<td>Zero Knowledge Proving</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 1: Major attack scenarios in WBAN.........................................................6
Table 2: RSA variable appendix.................................................................8
Table 3. Total combination and size comparison.......................................21
Table 4. Comparison of communication length of round trip with ECC protocols....21
Table 5. Kilinc’s computation time calculation table.....................................22
Table 6. Khan’s execution time calculation model [23] .................................23
Table 7. Computation cost comparison with ECC using Khan’s model..........23
Table 8. Attack Immunity comparison between ECC methods and TOKEN-PSRSA...24
LIST OF FIGURES

Figure 1. Wireless Body Area Network.................................................................3
Figure 2. Simple star topology example.................................................................5
Figure 3. How RSA Encryption Works.................................................................8
Figure 4. RSA Encryption Decryption Example.....................................................9
Figure 5. Sensor placement of on body simulation for evaluate protocol in real life.....13
Figure 6. PSRSA flow for Authentication............................................................15
Figure 7. PSRSA MAC and Data transfer communication order.............................16
Figure 8. Rekeying protocol overlooks.................................................................17
Figure 9. Rekey generation in TOKEN-PSRSA......................................................18
Figure 10. Star shaped network for TOKEN-PSRSA.............................................19
Figure 11. MitM attack simulation on TOKEN-PSRSA........................................21
Figure 12. Memory Flooding attack simulation on TOKEN-PSRSA......................21
LIST OF EQUATIONS

Equation 1: RSA Encryption [17] .................................................................8
Equation 2: Encryption key generation [17] ...............................................8
Equation 3: RSA Decryption [17] ...............................................................9
Equation 4: Decryption key generation [17] ..............................................9
Equation 5. Possible combination calculation for PSRSA..............................20
Equation 7. Kilinc’s computation time calculation for TOKEN-PSRSA...........22
ABSTRACT

LIGHT WEIGHT ENCRYPTION BASED SECURITY PACKAGE FOR
WIRELESS BODY AREA NETWORK
SANGWON SHIN
2021

As the demand of individual health monitoring rose, Wireless Body Area Networks (WBAN) are becoming highly distinctive within health applications. Nowadays, WBAN is much easier to access than what it used to be. However, due to WBAN’s limitation, properly sophisticated security protocols do not exist. As WBAN devices deal with sensitive data and could be used as a threat to the owner of the data or their family, securing individual devices is highly important. Despite the importance in securing data, existing WBAN security methods are focused on providing light weight security methods. This led to most security methods for WBAN providing partial security protocols, which left many possibilities in compromising the system.

This paper proposes full security protocol designed for wireless body area networks consisting of light weight data encryption, authentication, and re-keying methods. Encryption and authentication use a modified version of RSA Encryption called PSRSA, developed to be used within small systems such as WBAN. Authentication is performed by using encryption message authentication code (E-MAC) using PSRSA. Re-keying is performed with a method called tokening method. The experiment result and security analysis showed that the proposed approach is as light as the leading WBAN authentication method, ECC authentication, while preventing more attacks and providing smaller communication size which fulfills the highest NIST Authentication Assurance Level (AAL).
I. INTRODUCTION

Wireless Body Area Networks (WBANs) are small-scale networks centered on a human body [1]. WBANs consist of sensors or devices used for monitoring and transmitting physiological signals to specialized medical servers [2, 3]. With WBAN, it is possible to continuously monitor the patient’s medical status and in doing so, WBAN reduces risk of critical situations by detecting any change with attached sensors so the doctor may take the necessary actions to maintain the patient’s life [4]. Since WBAN deals with life dependent data, it requires reliable, trustworthy, and secure data gathering [5]. However, security and privacy issues exist in real application of WBANs [6]. This happens because information is transmitted wirelessly in an open channel, leading to vulnerabilities and threats [7].

To overcome security and privacy issues within WBAN, security methods must be implemented; however, a properly sophisticated security method does not exist within WBAN. [8]. As WBAN is also a type of computer system, using existing security method could be a solution, but as there are existing limitations on WBAN due to its size, existing security methods cannot be directly implemented without any modifications. Well known limitations in WBANs are power, memory, computational capability, and communication rate [9, 10]. Because of such limitations, instead of applying one or two security methodologies, it is best to apply protocols [11]. Protocols are packages of multiple security methods that can be applied to networks, and by doing so, it is possible to enhance the security of networks. To ensure the level of security within protocols, there is a guideline from the National Institute of Standards and Technology (NIST) called Authentication Insurance Level (AAL) [12]. AAL are set in 3 levels with AAL-3
as highest level. To satisfy AAL-3, security protocols are required with following
security methods: Authentication, Cryptography, Cryptographic key exchange protocol
and resistance to attacks of Man in the Middle (MitM), Verifier Impersonation, Verifier-
Compromise, Replay resistance, and Authentication Intent [12]. The use of multiple
security protocols is necessary to satisfy AAL-3 since there are no single security method
that can defend from them all.

Because of limitations within WBAN, it is challenging to apply full protocols, and
as such, most research proposes applying a lighter version of the existing security method.
This fulfills the AAL-2 security level, however there are a handful of AAL-3 satisfying
methods. The most common approach to apply is modifying Elliptic Curve Cryptography
(ECC) because of its lightness and high security assurance. As ECC is more suited for
authentication over encryption, to maintain the security level high enough, it requires use
of other security methods as well. [13]. Because of this, proposing AAL-2 satisfying
security methods were preferred than AAL-3 satisfying security methods. However,
AAL-2 is considered the minimum level of security, and most networks require having
AAL-3 for confident protection [12]. To satisfy AAL-3, instead of using ECC, the most
popular method in WBAN, which only provides authentication method, using encryption
method with Message Authentication Code (MAC) allows both authentication,
encryption, and also secure key exchange protocol. In this paper, I propose security
protocol for WBAN composed with PSRSA and token-based rekeying (TOKEN-PSRSA)
which satisfies AAL-3.

The rest of paper is organized as: Background, Related work, Methods, Results and
evaluation including security analysis and conclusion.
II. BACKGROUND

2.1 WIRELESS BODY AREA NETWORK

WBAN is referred to as a network formed with small sensor devices positioned on the body to collect medical data from user [1]. WBAN can be placed on various places of body to collect necessary data using medical sensors. This collected data will be sent to hospital or medical specialist, allowing them to monitor patients medical condition continuously, to aid specialists in specifying the health condition of the patient more closely or to detect emergency situation such as sudden heart attack or stroke [2]. Not only within health monitoring, use of WBAN is expanding rapidly also in multiple fields such as athlete training in monitoring athlete’s performance, and armed forces in monitoring the troops’ status. WBAN became more available to the public recently; smart watches and electronic sports monitoring bands are types of WBAN available in the market for anyone to purchase. Figure 1 shows the basics of WBAN formation with multiple sensor device, intermediate server and specialist to analyze the collected data such as doctors or hospitals.

![Figure 1. Wireless Body Area Network](image-url)
To be able to place sensors free of wires for WBAN, usually each sensor requires a small computing board with it such as Microchip, Microcontrollers or even FPGA. These are small computing board size from less than few millimeters to 10cm. Because of such size, there are various limitations, such as low in computation power, low in memory size, and low in communication power [9, 10]. Depending on purpose, WBAN’s can select the computing board from 3 different level of computations: Low, Medium, and High. Computation and size of the computing board get larger by higher computation levels and higher costs. Requirement of computation levels differs by the purpose of sensors as following:

1. Low computational

Nodes with low computational power are used for sensors to collect data with low frequency and disposable sensors such as blood glucose sensors. Such nodes are considered to have microchip for gathering and sending data to intermediate node that collects all the data’s prior to sending to server.

2. Medium computational

Nodes with medium computational power are used with sensors required in collecting data frequently such as pulse sensor, temperature, and others. Following nodes are considered to have computational power and size comparable of micro controllers, authentication, encryption, and decryption, which allows enough computation to handle gathering and storing of the data. Intermediate node also falls with medium computational nodes and gathers data from multiple sensors and sends it to High computational node for further processing.
3. High computational

Nodes with high computational power are used in storing data and processing it for final use. High computational node considers having computation power of regular PC, such as a laptop.

With the 3 given computational levels, most WBANs are formed in star topology. As shown in figure 2, star topology transmits all data to the central node, or the intermediate node, then the intermediate node transfers sanitized data to workstation. Using star topology allows individual sensors to use less power on communication and storing data and by limiting the long-distance communication allows to minimize the security compromise by use of open wireless transmission, making this approach as the most common approach taken within WBAN [14].

Figure 2. Simple star topology example

In this paper, TOKEN-PSRSA takes a similar star topology form as figure 2 shows.
2.2 SECURITY THREATS

Understanding security threats are important in understanding why security matters in WBAN, and why existing methods for WBAN are not secure enough. Major attack scenarios and how to handle it in WBAN are shown on table 1.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Requirements</th>
<th>Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthenticated access</td>
<td>Key establishment</td>
<td>Embedded key</td>
</tr>
<tr>
<td>Message disclosure</td>
<td>Confidentiality and privacy</td>
<td>Encrypting Authentication code</td>
</tr>
<tr>
<td>Denial of Service Flooding attacks</td>
<td>Availability</td>
<td>Blacklisting</td>
</tr>
<tr>
<td>Routing Attack</td>
<td>Secure routing</td>
<td>Authentication with Node ID checking</td>
</tr>
</tbody>
</table>

Table 1: Major attack scenarios in WBAN

Each threat shown in table 1 is critical for WBAN. Unauthenticated access will allow fake nodes to send and receive patient’s data. Message disclosure can conflict the server to modify patient’s status and can show that the patient is not in danger even if they are in peril. Denial of Service and flooding attacks can fill up memory of WBAN which results in halting the system or physically damaging the sensors. Threats scenario showed in table 1 falls into the following network threat categories:

Physical (Jamming, Tampering), Link (Collision, Unfairness, Exhaustion), Network (neglect and greed, Homing, Misdirection) and finally, transport (Flooding, Desynchronization). From these attacks, the goal of security in WBAN is to preserve Data confidentiality, data integrity and data freshness. Each represents how secure the data is, how trustworthy the data is, and finally how new the data is. By keeping these three categories from specified attacks, it is possible to keep WBAN secure [8].
2.3 DATA AUTHENTICATION AND ENCRYPTION

To satisfy NIST AAL-3, it is important to satisfy data authentication, encryption, and protection against certain attacks. Authentication is a method to grant or deny the access of incoming transmission. Through authentication, the device is required to prove that it is allowed to transmit within the network. Authentication is an important step to block any unwanted transmissions. There are multiple authentication methods; however, the TOKEN-PSRSA uses MAC with Encryption. MAC is a simple way of performing authentication. Once authentication is required from the receiver, the sender has to send MAC. Once the receiver receives MAC, it will compare with MAC it has. When the sent MAC matches with MAC that the receiver has, MAC will grant the sender access to the network. Because it is simple, this process does not require much computation power. However, to prevent MAC getting hijacked in the middle of transmission, MAC is required to be encrypted. There are many encryption methods that one can apply to create E-MAC; however, with proposed method, I have chosen to use RSA encryption.

RSA is one common encryption that is widely used within many forms of networks [15]. However, it is considered as not suitable to be used within WBAN, because RSA requires key size more than 1024 bit to be secure, which means RSA is heavy in size [15, 16]. Original RSA is Asymmetric encryption, meaning RSA has separate encryption and decryption key. Encryption keys are sent to the public, but the encryption keys cannot be used to decrypt the message. Decryption keys are kept secret, and are called private keys. Because of this method, RSA can be used to encrypt against multiple sender and single receiver while sender cannot use their key to decrypt what anyone in network sent to the receiver. RSA is widely used since most network servers
are formed in multiple senders to a single receiver. Figure 3 explains process of RSA encryption. First using public key, sender encrypts the data with public key. Once the data is encrypted, this will be sent to receiver. Receiver will then use a private key to decrypt the RSA encrypted data. Public keys are open keys sent out by the receiver, and private key is a secret key only kept by the receiver.

![Figure 3. How RSA Encryption Works](image)

RSA encrypts the data using modular exponent calculation. Encryption equation of RSA is as follows:

\[
c = m^e \pmod{n}
\]

Equation 1: RSA Encryption [17]
to generate encryption key, the following equation is used:

\[ \lambda(n) = lcm(p - 1, q - 1) \]

Equation 2: Encryption key generation [17]

Where prime number p and q cannot be equal number, and exponent e in Equation 1 must satisfy \( \gcd(\lambda(n), e) = 1 \); \( 1 < e < \lambda(n) \) to be able to decrypt [17].

To decrypt the RSA encrypted data, following equation will be used:

\[ m = c^d \mod n \]

Equation 3: RSA Decryption [17]

where decryption key d is determined using exponent and prime number used to encrypt as following:

\[ e \cdot d = 1 \mod ((p - 1) \cdot (q - 1)) \]

Equation 4: Decryption key generation [17]

Figure 4 shows actual RSA encryption and decryption process
2.4 SECURITY PROTOCOL

To be able to secure WBAN with satisfying NIST AAL-3, WBAN requires security protocol [11]. Security protocol is the series of security methods gathered, forming one package. For example, security protocol can be formed with authentication and encryption. Use of multiple security protocols allows for enhanced security over using single security method, since each security method has weaknesses. Security protocol are formed to cover each security methods’ weakness, which results in providing secure networks. Within WBAN, there are not many proper security protocols proposed, and because of this, many proposed protocols have multiple weaknesses which allows for systems to be compromised. In the proposed method, Security protocol are formed with MAC Authentication, PSRSA Encryption, and Token based re-keying method. By providing 3 security methodology, it is possible to satisfy NIST AAL-3 requirement which assures secureness of proposed protocol.
III. RELATED WORK

There exist multiple threats that can compromise WBAN, and before implementing security methods, it is important to understand what the threats for WBAN are.

Niksaz et al [18] proposed possible threats and attacks for WBAN with possible counter measures. Niksaz has defined attack layers and multiple scenarios of possible attacks on WBAN, which can be used to check that the security methods are secure against attack scenarios. There are multiple ways to secure WBAN. Most common approach taken is to use ECC and implement authentication. Izza et al [7] proposed WBAN with ECC. In this model MAC is used along ECC and has resistance to replay attack and Denial of Service (DoS). Kumar et al [19] proposed secure authentication protocol using ECC and SHA hash function. There are multiple other ECC based methodologies to secure WBAN, because ECC is light and has strong security. However, ECC is an authentication method rather than an encryption method. Because of this, ECC requires separate encryption methods to secure the data transmission. Other common proposed approach is using Zero Knowledge Proving (ZKP). Ma et al [20] proposes a TinyZKP, a lightweight protocol of ZKP for authentication. ZKP is used to encrypt the secret information of SHA-1. However, ZKP requires multiple communications to gain authentication, since ZKP requires self-proving based on questions asked by server, which results in higher communication cost.

While ECC and ZKP are common methods to provide security to WBAN, RSA is a very rare selection for WBAN because the size of RSA is heavy in memory and computation. However, RSA can provide both authentication using MAC and data
encryption, while both ECC and ZKP can used for authentication but not for encryption. Using RSA in WBAN is rare but it is possible. Chang et al [16] proposed a partial RSA signature scheme based on periodical re-keying for wireless sensor networks. To reduce the size of RSA to fit into WBAN, key size has been reduced, while using re-keying method allowed to keep security level. In this method, RSA Key is rekeyed per time T. Both WBAN and Server hold pools of pre-implemented small keys and change keys, however once the keys are all used, the following protocol re-uses the previously used keys which leads to security weakness. Aarti et al [21] proposed hybrid models for use in clustered WBAN. This method uses RSA and SHA together. Most of the proposed methods above can satisfy NIST AAL-2, however because most of them are partial security packages, they cannot achieve NIST AAL-3 and there are numerous weaknesses to compromise the network.
IV. METHODS

TOKEN-PSRSA is formed with 2 main parts. The first part is PSRSA, and the second is token-like rekeying protocol using PSRSA. Combining two methods allows the satisfaction of the NIST AAL-3 security level. To evaluate the protocol, simulation has been taken using 5 Arduino microcontrollers with choice of electromyography, flex, temperature and pulse sensors to simulate performance of the protocol within real life usage.

Figure 5. Sensor placement on body simulation for evaluating protocol in real life
4.1 PREPROCESSED SYMMETRIC RSA

Applying RSA encryption, to currently existing WBAN nodes composed of microcontrollers, requires modification due to WBANs limitations [9, 10]. However, simply reducing the size of RSA results in lowering the security level [16]. To avoid lowering security level, proposed method adds preprocessing layer in front of RSA. Due to the asymmetric method of RSA, and the size of key, communication costs are not very effective since asymmetric requires public key distribution [8]. To reduce the communication cost, simply implementing key generation processes into sensor nodes allows the nodes to generate encryption keys. Doing so is also important to perform re-keying protocol to maintain security level.

Adding preprocessing layers will promise the increase of security, with the cost of more computational power. To avoid such problems, algorithms used in preprocessing layers require having lower computation time than RSA encryption and decryption. By doing so, we can maintain computation time of RSA with smaller keys and still maintain required security levels to secure the network. Preprocessing layers are composed with added mix key, padding message, and bit shifting or bit operation. PSRSA allows choice of preprocessing by bit shifting or bit operation. This leads to an increase of possible combinations, which results in an increase of security level. Mix key layer has 256-bit unique key that is pre-implemented in nodes, and uses this key to mix into message. Once the message is mixed, mixed message will be then sent to the padding phase. The padding phase will pad the message with pre-implemented padding pattern. Once message is padded, based on the user’s choice, PSRSA will perform bit shifting or reversible bit operation such as XOR, NOT or XNOR. Once preprocessing of message is
over, then it will be sent to Symmetric RSA to be encrypted. The encrypted message will be then sent over to an intermediate node, which decrypts it exactly the opposite of PSRSA encryption.

Since PSRSA is an encryption methodology, it is possible to use it as authentication with MAC. Using MAC will go through the same process with data, with the only difference being encrypting data or authentication code. Because we have one encryption method for both data encryption and authentication, this allows us to have a full security package while maintaining the small size of the security package compared to other methods such as ZKP or ECC, since both ZKP and ECC cannot be used for data encryption while RSA can be used in both. Figure 6 shows logic flow of PSRSA with MAC for authentication.

![Diagram of PSRSA flow for Authentication](image-url)

Figure 6. PSRSA flow for Authentication
Figure 7 shows a detailed overlook of PSRSA logic flow between sensor and intermediate node. Once authentication is requested, intermediate node asks sensor to provide the authentication key. Using pre-implemented information, sensor now encrypts authentication message using PSRSA and sends it to the intermediate node. When the intermediate node receives PSRSA encrypted key, it will send grant message to sensor. Once the sensor is granted to transmit data, the sensor sends encrypted data using PSRSA to the intermediate node and the intermediate node will decrypt and store the received data.

![Diagram of PSRSA MAC and Data transfer communication order](image-url)

**Sensor node**
- bo(x) = bit operation
- si(x) = bit shift
- pm = preprocessed message
- mk = mix key
- c = encrypted message
- e = exponent
- mk = mix key
- p, q = prime number
- pb = pad bit

\[
x = MAC + mk + pb
\]
\[
pm = si(x) \text{ or } bo(x)
\]
\[
c = pm^e \mod (p \cdot q)
\]
\[
y = DATA + mk + pb
\]
\[
Dpm = si(y) \text{ or } bo(y)
\]
\[
ED = Dpm^e \mod (p \cdot q)
\]

**Intermediate node**
- bo\(^{-1}\)(x) = inverse bit operation
- si\(^{-1}\)(x) = inverse bit shift
- pm = preprocessed message
- mk = mix key
- c = encrypted message
- e = exponent
- p, q = prime number
- pb = pad bit

\[
\text{Grant}
\]
\[
pm = c \cdot \frac{(p-1) \cdot (q-1)}{e} \mod (p \cdot q)
\]
\[
x = bo^{-1}(pm) \text{ or } si^{-1}(pm)
\]
\[
MAC_x = x - pb - mk
\]
\[
\text{if } (MAC_x == MAC)
\]
\[
\text{Authenticate}
\]
\[
\text{Decrypt ED using PSRSA}
\]

Figure 7. PSRSA MAC and Data transfer communication order
4.2 RE-KEYING PROTOCOL

Using PSRSA provides both authentication and data encryption. However, PSRSA carries the same weakness of RSA. To secure the network further requires re-keying. Re-keying the PSRSA encryption and decryption key will enhance the security levels, allowing for network security. Re-keying requires sending new key information from intermediate node to sensor. However, when a new key information is sent through the wireless networks, the key is then opened, resulting in neutralizing security of the entire network. We can prevent such a problem by encrypting new key generating information with PSRSA which allows safe re-keying method. To do so, both sensor and intermediate require having pre-made master key purposed to decrypt only new key generating information as needed.

Figure 8. Rekeying protocol overlooks
As shown on figure 8, when sensor sends expired encryption key, instead of a grant message, it sends a new encryption key that has been encrypted with PSRSA using master key. Once the sensor decrypts the new key using master key, the previous key will be overwritten with the new encryption key and be re-sent with it. To perform rekeying in proposed manner, protocol requires a way to expire the old key. One common approach is trying to synchronize two device using timestamps. However, the synchronization of two devices has a high computation cost. To be able to expire the old key, TOKEN-PSRSA uses web tokening approach like the approach of Jason Web Token.

Tokening allows us to renew the information without synchronizing. Tokening is defined as encrypted key including data and changeable information like session or timestamp. Because the tokening key requires encryption, re-generated key will be kept secret. TOKEN-PSRSA re-generates a key by taking the previous key, mixing it with randomly generated simple session in intermediate node and the timestamp of key generation. Intermediate node keeps the timestamp of the generated key and will expire the key once the expiration time is over. Every time a key generates it has a new session and a new timestamp, resulting in a new key; and since the old key will not be in use anymore, tokening can prevent many security attacks.

![Rekey generation in TOKEN-PSRSA](image)

Figure 9. Rekey generation in TOKEN-PSRSA
V. RESULTS AND EVALUATION

To simulate and prove the TOKEN-PSRSA is a protocol that fits and satisfies AAL-3, TOKEN-PSRSA has been implemented into an Arduino feather micro-controller with the following specs: 80Mhz clock speed, 4MB Storage, 50KB Memory with ESP8266 communication module on board. The following microcontroller will be considered a node with medium computation level and communication power, which is consistent for most of the nodes that WBAN networks are composed of. Using micro-controllers, WBAN is formed in star-shaped network. Figure 10 below shows the basic structure of star shaped network for TOKEN-PSRSA.

![Diagram of star shaped network for TOKEN-PSRSA](image)

Figure 10. Star shaped network for TOKEN-PSRSA

All sensor nodes are required to communicate to hub node, and to communicate from low computation nodes. Because of its limited computation and communication power, low computation nodes are required to communicate with medium computation power nodes. Medium computation node will transmit the information sent from low computation node and pass it through to the Hub node with PSRSA data encryption. Once hub nodes gain...
enough information from sensor nodes, hub nodes will follow TOKEN-PSRSA protocol and send the chunk of information to server.

Using the network above, TOKEN-PSRSA had tests to check its availability for use in WBAN and performed simulation for attack scenarios to check its durability and satisfy the AAL3. Availability simulation was taken with the following durations and running full protocol including TOKEN based re-keying: Short term of 10 minutes, Long term of 2 hours and 1 day continuously running authentication. In the availability simulations, there were no authentication failures or memory overflow issues. Subsequently, it is possible to conclude proposed protocol, TOKEN-PSRSA, is fit for WBAN with star shape.

Through simulation, TOKEN-PSRSA has proven as fit to be used for WBAN. However, there is still a need to evaluate the security assurance of the proposed protocol. To do so, providing the theoretical and mathematically proven data is necessary. It also must perform attacks on the networks to prove the immunity on certain attacks to satisfy AAL-3. First, security attack simulation was taken to the network with protocol for one week using laptop PC with Core-i7 CPU. Types of attack performed are followed by NIST AAL guideline [12] and specified result per attack will be shown in the table below. Figure 11 below shows the attack simulation to network with brute force on authentication key based on man-in-the-middle scenario, and Figure 12 shows the message flooding attack.
Figure 11. MitM attack simulation on TOKEN-PSRSA

Figure 12. Memory Flooding attack simulation on TOKEN-PSRSA
To ensure the security level of TOKEN-PSRSA protocol is reached to the expectation, security analysis has been taken as a proof of theoretical and mathematical assurance for the protocol. Proposed model depends heavily on having high security level with PSRSA. Encryption, depending on how many possible combinations exist, shows how secure the algorithm is [22]. PSRSA generated combinations can be calculated using following equation 5:

\[
\text{Combination} = \frac{2^{nk}}{\ln (2^{nk})} \ast 6 \ast sb \ast kb \ast P(kb, 94)
\]

Equation 5. Possible combination calculation for PSRSA

Within equation 5, nk represents the number of digits, 6 as number of bit shifting and bit operation candidate possible to choose, sb as size of bit key used for bit operations, kb as the bit size of mix key, taking permutation will give result for possible candidate of characters from 94 characters in ASCII code.

Along with combination calculation, determining security level is required to prove the security level. RSA family security level is calculated with General Number Field Sieve (GNFS) as shown in equation 6.

\[
\text{Security Level of RSA} = \exp \left( \frac{3}{9} \left( \sqrt[3]{\frac{64}{9}} + O(1) \right) (\ln(n))^{\frac{1}{3}} \ast (\ln(\ln(n)))^{\frac{2}{3}} \right)
\]


Using the equation above, we can derive PSRSA possible combinations and compare with other RSA based method and ECC, the most commonly used method in WBAN for security.
Table 3. Total combination and size comparison

Comparing Key size, PSRSA was able to reduce from 1024 bit to 256 bit from original RSA and able to maintain security level of 80 bits. PSRSA was able to have total combination of $10^{372}$ which is higher than original RSA and ECC with same security level. PSRSA total combination is very close to 1024 bit RSA with SHA.

Next, we compare the communication cost of the entire protocol based on round-trip length. Round-trip length shows how many bits are required to gain authentication.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Communication cost Length (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Khan J et al [23]</td>
<td>4288</td>
</tr>
<tr>
<td>D. He, et al [24]</td>
<td>5328</td>
</tr>
<tr>
<td>X. Jia et al [25]</td>
<td>6672</td>
</tr>
<tr>
<td>K. Sowjanya et al [26]</td>
<td>3264</td>
</tr>
<tr>
<td>M. Nikooghadam et al [27]</td>
<td>3440</td>
</tr>
<tr>
<td>TOKEN-PSRSA</td>
<td>768</td>
</tr>
</tbody>
</table>

Table 4. Comparison of communication length of round trip with ECC protocols

Compared to other ECC protocols for WBAN, TOKEN-PSRSA has significantly less communication cost based on comparing communication length. This is because RSA does not require much information to be encrypted or to be decrypted, and because ECC requires multiple information requests to process authentication.
Another important factor to consider for protocol is execution time within WBAN.

To calculate the TOKEN-PSRSA execution time in milli-second, Kilinc et al [28] calculation model is used. Table 5 shows the computation time calculation table.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Operation</th>
<th>Arithmetic Mean (ms)</th>
<th>Standard Deviation (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RNG</td>
<td>Select random number $Z_r$</td>
<td>0.539</td>
<td>0.0000106</td>
</tr>
<tr>
<td>H</td>
<td>String to number (hash) $Z_r$</td>
<td>0.0023</td>
<td>0.0000006</td>
</tr>
<tr>
<td>$H_1$</td>
<td>String to point (hash) $G_1$</td>
<td>12.418</td>
<td>0.0000442</td>
</tr>
<tr>
<td>$H_2$</td>
<td>String to point (hash) $G_2$</td>
<td>0.3947</td>
<td>0.0000260</td>
</tr>
<tr>
<td>PM</td>
<td>Point multiplication $G_2$</td>
<td>2.216</td>
<td>0.0000733</td>
</tr>
<tr>
<td>PA</td>
<td>Point addition $G_1$</td>
<td>0.0288</td>
<td>0.0000025</td>
</tr>
<tr>
<td>PAIRING</td>
<td>Pairing $G_1 \times G_1 \rightarrow G_2$</td>
<td>5.811</td>
<td>0.0002854</td>
</tr>
<tr>
<td>ID-SIGN</td>
<td>Id Based Signature (Hess)</td>
<td>23.8662</td>
<td>0.003236</td>
</tr>
<tr>
<td>ID-SVER</td>
<td>Id Based Verification (Hess)</td>
<td>5.87147</td>
<td>0.001007</td>
</tr>
<tr>
<td>EXPO</td>
<td>Modular exponentiation (1024 bit)</td>
<td>3.850</td>
<td>0.0000464</td>
</tr>
<tr>
<td>SIGN</td>
<td>RSA Signature Func. (1stEXPO)</td>
<td>3.8500</td>
<td></td>
</tr>
<tr>
<td>SVER</td>
<td>RSA Verification Func. (EXPO/20)</td>
<td>0.1925</td>
<td></td>
</tr>
<tr>
<td>ENCB</td>
<td>Block Cipher Encryption (2ndH)</td>
<td>0.0046</td>
<td></td>
</tr>
<tr>
<td>DECB</td>
<td>Block Cipher Decryption (2ndH)</td>
<td>0.0046</td>
<td></td>
</tr>
<tr>
<td>ENCP</td>
<td>Public Key Encryption (1stEXPO)</td>
<td>3.8500</td>
<td></td>
</tr>
<tr>
<td>DECP</td>
<td>Public Key Decryption (1stEXPO)</td>
<td>3.8500</td>
<td></td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash-based Message Authentication Code (2ndH)</td>
<td>0.0046</td>
<td></td>
</tr>
</tbody>
</table>

Table 5. Kilinc’s computation time calculation table [28]

Using Kilinc’s computation time calculation table, TOKEN-PSRSA will have following equation:

$$TOKEN - PSRSA: 4H + 2SVER + 2ENCP + 2DECP + 2HMAC = 15.79 \text{ ms}$$

Equation 7. Kilinc’s computation time calculation for TOKEN-PSRSA

Adopting the table above for ECC results in 13ms. TOKEN-PSRSA is only 2ms slower compare to most used method for authentication. However, Kilinc’s model is suitable to encryption methods, and as ECC is an authentication method; adopting Kilinc’s table may produce error.

Another calculation method to apply is Khan et al [23] calculation model.

Table 6 shows Khan’s execution time calculation model.
Table 6. Khan’s execution time calculation model [23]

Within Table 6, ECC-based multiplication and point addition has same algorithm with regular multiplication and point addition, allowing for the calculation of TOKEN-PSRSA execution time. Using Table 6, we get following equations for TOKEN-PSRSA:

\[
\text{TOKEN - PSRSA SERVER: } T_A + 2T_I + T_M + T_E + 2T_SM = 0.949 \text{ ms}
\]

\[
\text{TOKEN - PSRSA SENSOR: } 2 \times (T_A + 2T_I + T_M + T_E + 2T_SM) = 1.898 \text{ ms}
\]

By adding two worst case execution time calculated, results show TOKEN-PSRSA has 2.85ms according to Khan’s execution time calculation model. Table 7 has comparison of computation cost between ECC methods. Most ECC based methods have similar or slower execution times than TOKEN-PSRSA.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Computation cost (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Khan J et al [23]</td>
<td>Sensor/Client + Server</td>
</tr>
<tr>
<td>X. Jia et al [25]</td>
<td>8.069</td>
</tr>
<tr>
<td>K. Sowjanya et al [26]</td>
<td>2.79</td>
</tr>
<tr>
<td>M. Nikooghadam et al [27]</td>
<td>2.19</td>
</tr>
<tr>
<td>TOKEN-PSRSA</td>
<td>2.85</td>
</tr>
</tbody>
</table>

Table 7. Computation cost comparison with ECC using Khan’s model
The last element to analyze before concluding the safeness and efficiency of TOKEN-PSRSA for WBAN is comparing what kind of attacks are preventable. To satisfy NIST AAL-3, protocol requires immunity to attacks specified in guideline [12].

Using scenarios proposed in guideline and categorization for WBAN threats, Table 8 below is generated.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Replay</td>
<td>-</td>
<td>-</td>
<td>○</td>
</tr>
<tr>
<td>MitM</td>
<td>-</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>DoS</td>
<td>-</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Known key</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Perfect forward</td>
<td>-</td>
<td>-</td>
<td>○</td>
</tr>
<tr>
<td>Verifier impersonation</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Authentication intent</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

Table 8. Attack Immunity comparison between ECC methods and TOKEN-PSRSA
VI. CONCLUSION

WBAN is a rapidly growing technology because of its convenience and possibilities for monitoring patient’s health data at any time [8]. WBAN deals with life critical data and privacy which requires security methods [6]. However, within WBAN, there is not a properly sophisticated security method in existence [8]. Limitations to the use of existing security methods are WBAN’s limitation on power, memory, computational capability, and communication rate [9, 10]. To ensure secureness of WBAN requires modifying existing security methods and acquiring NIST AAL-3 [12]. This paper proposed TOKEN-PSRSA, a security package composed with authentication, encryption, and re-keying. Key component of protocol is RSA encryption modified to be symmetric RSA with preprocessing layer, PSRSA and E-MAC authentication using PSRSA. TOKEN-PSRSA have proven efficient in speed and in size, along with immunity to multiple cyber-attacks using calculation and threats simulation. Results of analysis and simulation shows TOKEN-PSRSA satisfies NIST AAL-3.

Even though TOKEN-PSRSA is aimed for network security within WBAN, it could also be applied to other small systems. Since TOKEN-PSRSA protocol satisfies the NIST AAL-3 assurance level within small systems such as WBAN, the possibility of applying the same protocol to secure the other types of small system networks is possible throughout multiple other applications such as Internet of Things (IoT) and Vehicle networking.

Next step of work is to improve re-keying method to be more effective. While the proposed protocol’s re-keying method is efficient compared to other methodology, it is
possible to make a more efficient re-keying process by reducing communication numbers, or by changing the re-keying method to another method.
VII. LITERATURE CITED


[16] Shih-Ying Chang, Yue-Hsun Lin, Hung-Min Sun, and Mu-En Wu. Practical rsa
signature scheme based on periodical rekeying for wireless sensor networks ACM

signatures and public-key cryptosystems. Communications of the ACM, 21(2):120-

[18] Pejman Niksaz and Mashhad Branch. Wireless body area networks: attacks and

for wearable devices environment using ecc. Journal of Information Security and

[20] LImin Ma, Yu Ge, and Yuesheng Zhu. Tinyzkp: a lightweight authentication scheme
based on zero-knowledge proof for wireless body area networks. Wireless personal

[21] Aarti Sangwan and Partha Pratim Bhattacharya. A hybrid cryptography and
authentication based security model for clustered wban. JOURNAL OF
MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, 13(1):34-54,
2018.

[22] Steve Burnett and Stephen Paine. The RSA security’s official guide to cryptography


