Mutual Authentication in Body Area Networks (BANs) Using Multi-Biometric and Physiological Signal-Based Key Agreement

Nur Adibah Saffa, Fiona Anne Angkoi, Alice Bangi Pang, Lydia anak Kendawang, Sherilina Luense, Sonia Miana Cyril Ondoi and George Dinggat David Among
Faculty of Computer Science and Information System, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
email: *adibasaffa98gmail.com

Date received: 25 August 2021
Date accepted: 1 November 2021
Date published: 30 November 2021

Abstract - *The development of wireless technology has had a major impact on the wireless body area networks (WBANs) especially in the medical field where a small wireless sensor is installed in, on, or around the patient's body for real-time health monitoring and personalized medical treatment. However, the data is collected by the sensors and transmitted via wireless channels. This could make the channel vulnerable to being accessed and falsified by an unauthorized user and may put the lives of the patient at risk and might give a false alarm. Therefore, a secure authentication and data encryption scheme in BANs is needed in a device to establish the interaction. The asymmetric cryptosystems that function in BANs can cause a Man-in-the-Middle attack because the initial requirement in BAN requires the user to configure a master key or password. The impersonation attack may also involve BAN where other individual pretends to be the owner of the devices and lastly Eavesdropping attack where the attack eavesdrops on transmission to unlock devices. With the existing schemes, mutual authentication using the biometric features (fingerprint) and the physiological signal from the electrocardiogram database is used to make sure the authentication is more secure, reliable, and accurate. In this paper, we proposed a new multifactor authentication scheme on biometric authentication which is the retina scan. We proposed the retina scan because the retina of the human eye is unique, remains the same, and cannot be obtained from anywhere which makes it difficult to forge. We also added a new device which is a smart watch to receive a key agreement message from the fingerprint to double confirm the same identification. This is to make sure high security is obtained and offered simplicity, efficiency, and precision scheme for the authentication.*

Keywords: Body area network (BANs), secure communication, biometric-based security, physiological signal, key agreement.

1 Introduction

Mutual authentication and specifically multifactor authentication mechanism are not a new research paradigm. Several researchers have proposed several methods to ensure secure authentication mechanisms in any communication protocols (Balan et al., 2018; Khan et al., 2019)

Wireless technology becomes more popular because of its flexibility and ability to solve problems in various application domains. This technology presents different ways to ease and assist society in daily life such as military applications, area monitoring, transportation, and health applications (Sridhar et al., 2020). The development of wireless technology gives great impacts on human life especially in the medical field where the wireless body area networks (WBANS) are included and the monitoring of patient-healthcare through the internet is possible (Alzahrani et al., 2020). Wireless body area networks (WBANS) are significant for the

monitoring applications in healthcare lifestyle which involve the transmission of health data and constant approach to the patients.

However, the reliance on wireless technology can lead to some security problems in BAN where this involves private or personal health data. The wireless channels for the transmission of health data collected by the sensors can cause data vulnerability and unauthorized user access. This situation can risk the life of the patient and lead to a false alarm. This will cost the patient's information to be altered where it can lead to wrong diagnosis results. Thus, a secure communication and data encryption scheme between BANs should exist which includes the authentication between the devices to form the interaction.

The existing schemes proposed an agreement scheme for BAN that includes mutual authentication using a biometric feature which is fingerprint. The physiological signal from the electrocardiogram database was also included to increase the security and reliability in the authentication and communication between the devices of BAN. In this paper, we proposed a new multifactor authentication scheme where we proposed an additional feature for biometric authentication which is retina scan. Retina plays a significant role especially in the individual's automatic recognition which can help in improving security and limiting access to the system and this biometric verification technique is proven to be more competent than the fingerprint technique (Roy et al., 2019). The retina scan was chosen in this paper because of the difficulty to be forged as the patterns are unique thus, this can produce a reliable biometric authentication system. Along with the retina scan, we also proposed a new device which is a smartwatch to double confirm the same identification where the watch will receive key agreement message from the fingerprint, thus high security can be achieved.

The methods to solve the problems include the combination of the retina and fingerprint scan with the involvement of mobile devices and smartwatches to provide high security in the authentication process. When the retina is scanned, this will input the image, and preprocessing will occur. Preprocessing includes green channel extraction, background extraction, and noise removal mask. Next, vascular pattern extraction will be performed which includes blood vessel enhancement and segmentation, then the features will be extracted and validated. Feature matching will occur which includes test feature extraction and feature vector in the database until the image is recognized. The Health app will only display a summary from the previous calculated activities by the smartwatch. For the user to access further details of the calculated activities by the smartwatch, the user must input the fingerprint. The sensor will initiate the authentication and a random key will be generated using a fuzzy commitment algorithm (Dharanesh et al., 2017). If the real-time psychological signal is successfully captured, the key agreement message will be sent to the receiver. The receiver will use its protected key to unlock the vault and if it is correct, the receiver will acknowledge the authenticator (Dharanesh et al., 2017).

Although there might be existing authentic systems that supported biometrics technology, however, it can be denied that all of those technologies can be forged by the attacker. The security analysis for our proposed solution aims to tighten the security and robustness against any attacks. Man-in-the-middle happened when a stranger tried to steal or fabricate the data. The attacker is unable to recreate a similar key in the sniffing process since the proposed solution implemented fuzzy commitment protection and fuzzy fault protection. The next attack is node impersonation. Nowadays, the attacker can duplicate data. Our proposed solution can break the node impersonation since the attacker will have a lot to do which is very time-consuming to find the match of the biometrics. Since the retina of the human eye is unique, it is difficult to forge. The last attack is eavesdropping. It has a variety combination of properties that makes the attacker unable to identify the perfect match of the properties combination.

For the authentication overhead and computational overhead, although have three authentication moods, the proposed scheme still has a lower computational overhead compared to the existing solution. As for authentication overhead, it is calculated around 1600 bits. In this paper, we proposed a secure and efficient scheme authentication The main contributions of the paper are outlined as follows:

i. We proposed a new multifactor authentication scheme with an additional feature for biometric authentication; retina scan
ii. We analyze the security characteristic of our proposed solution that can withstand various attacks such as man-in-the-middle attacks, node impersonation, and eavesdropping.

Secure and accurate access control is essential. These approaches offer simplicity, efficiency, and precision assume the same level of security to all applications and fall short on delivering authentication beyond the point of entry (Abuhamad et al., 2021). Moreover, these biometrics approaches require overt recognition, where the user explicitly enters the unique password or used biometrics, making them fail in delivering implicit,

transparent, and continuous authentication. Despite the alternatives of using biometrics technology as an authentication measure, some are still attacked by many challenges that lead to system performance degradation concerning identification time and accuracy (Adetunji et al., 2018) . Though these problems have been tackled by many researchers using different techniques to enhance the overall identification system performance, the ideal solutions for some of these problems are still unavailable.

The proposed work can be extended to enhance end to end security mechanisms in network intrusion detection systems or malware detection systems (Ji et al., 2018; A. S. Khan, Ahmad, et al., 2021; N. Khan et al., 2017).

2 Related Work

A variety of issues related to the security of the wireless communication in BANs such as the security authentications that had been proposed to stop the attackers from being able to access and falsify the data of the patients. Seven articles have been studied to improve the security of the data which include the methods used, the evaluation metrics, computational cost and authentication overhead, challenges, and the future direction.

A study proposed a new agreement scheme for BAN known as Multi-Biometric and Phycological Signal-Based Key Agreement (MBPSKA). The MBPSKA imposed both biometric characteristics and time-variant psychological signs on its user to create double lock security. Security breaches or attacks will cost patients' information to be altered which could result from the wrong diagnosis. There must be secure communication between BANs where each device must authenticate to each other to establish the interaction. In some cases, the patient who lost consciousness won't be able to give their consent during an emergency; a secure, reliable, and flexible scheme is needed for mutual authentications in a BAN. The MBPSKA scheme can defend devices from numerous attacks such as brute force attacks – the process of recreating the Binarized Phase Spectrum (BIPS) for example fingerprint, eavesdropping – an attack where eavesdrop on transmission to unlock devices, impersonations – other individual pretends to be the owner of the devices, man-in-the-middle-attacks – perpetrator can position himself between the devices and owner, and lastly replay attacks is an attack on the transmission which can lead to slow device performance. There are five (5) methods to mitigate the attacks as stated earlier. One of the methods is the Security of Fingerprint-Based Fuzzy Commitment – a process of obtaining probability distribution of the fingerprints together with the fuzzy commitment scheme by identifying the similarity of fingerprint impression. The second method is the Security of ECG-Based Fuzzy Vault – this process involves polynomial construction where hidden chaff points will be generated randomly to prevent. from any attacks. The higher the degree polynomial, the stronger the security strength. The third method to mitigate the attack is through Confidentiality – preventing unauthorized disclosure to the attacker. This method requires methods one and second which have been discussed earlier where the cryptographic session key will be exchanged between the methods if the authentication success the future messages is encrypted. The fourth method is Authenticity- refer to the user that receives data that is trusted and genuine. This is where methods one and two mention earlier provides safe and mutual authentication between the sender and receiver. The last method is integrity – this refers to the message that is not changed or modified during transmission. The message is hashed to protect from being altered. The MBPSKA scheme's aim in the future is to experiment with the real world to validate its design and plans to evaluate computation and memory cost.

A study by Ji et al. (2018) is proposing an efficient and certificateless conditional privacy-preserving authentication scheme for WBANs big data services to guarantee patients' security and their physiological data. This concept is planned to implement conditional privacy-preserving for the clients after they found that a number of the previous schemes failed to satisfy the protection needs and promise safer WBANs compared to alternative schemes. The proposed scheme in this article provides anonymity, un-linkability, mutual authentication, traceability, session key establishment, forward secrecy, and attack resistance. The authors claimed that it is more secure compared to the previous study and can satisfy all the safety requirements needed. The proposed scheme also attacks resistance, which can resist the reply attack, impersonation attack, modification attack, lost personal digital assistance (PDA) attack, and man-in-the-middle attack (Ji et al., 2018). The proposed scheme is divided into several crucial parts which are the system initialization phase, pseudo-identity generation and message signing phase, authentication phase; 1) individual authentication of a single client and 2) batch authentication of multiple clients, and the past phase is password change phase. The computational cost for the proposed WBAN scheme is the total computational cost of the client and application provider (AP). For the client, it will compute 3Tm for the execution time. While the execution time for AP is (4n+2) Tm. The proposed scheme is primarily based totally on elliptic curve cryptography and there is no bilinear pairing. Which successfully reduces the computational cost. The simulation test demonstrates that the proposed scheme is extra green and highly practical. By using pairing-based cryptography (PBC) to compute the running of the above cryptographic operations resulting the execution time are T_m = 2.576ms, T_e = 3.857ms

and T_p = 4.163ms where, T_m denotes the execution time of one scalar multiplication operation, T_e denotes the execution time of one exponentiation operation, and T_p denotes the execution time of one bilinear pairing operation. In a nutshell, an efficient and certificateless conditional privacy-preserving authentication scheme for WBANs big data services is proposed since there is no anonymous authentication scheme for WBANs that supports conditional privacy-preserving for the client. The purpose of this project is that to reduce the computational cost for the application provider, the proposed scheme can satisfy batch authentication of multiple clients at the same time (Ji et al., 2018). Based on Figure 1, it is seen that the proposed scheme offers a better computational time compared to the recent two authentication schemes for WBANs.

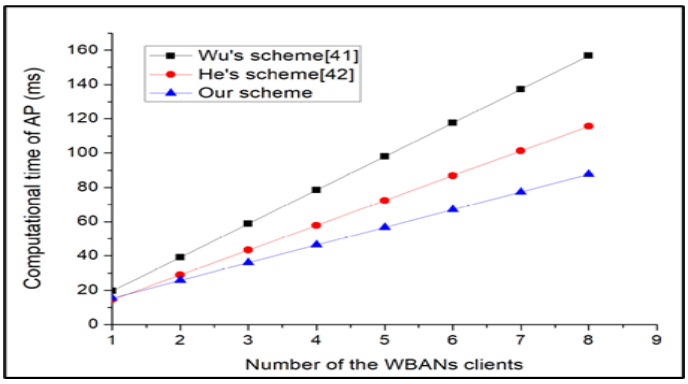

Figure 1: Computation time of AP refers to the number of the WBANs clients (Jafer et al., 2020)

There are many MAKA: mutual authentication and key agreement schemes have been presented over the years to protect user health information. Even though the WBANs and WSNs bring many benefits to the patients, but the services are vulnerable to many potential attacks. With that, Park et al. (2020) proposed a provably secure and lightweight MAKA scheme for medical IoT, called LAKS Non-verification table (NVT). As the name indicates, a server verification table is not required in LAKS-NVT. The proposed scheme is divided into three phases: a) "initialization phase," b) "registration phase," and c) "MAKA phase". The proposed scheme is examined for potential attacks such as stolen server node (SN) attack, impersonation attack, replay attack, anonymity and untraceability, secret mutual authentication (MA), and leaking verification table attack in the analysis of formal security. Real-or-random (ROR) model is used as a mathematical security analysis to prove session key security, and Burrows-Abadi-Needham (BAN) logic is used to verify that LAKS-NVT provides secure MA. In addition, a software tool the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" is used to ensure that the LAKS-NVT is secure against the aforementioned potential attacks. When comparing communication and computational costs, the authentication and key agreement phase for LAKS-NVT and other compared schemes are taken into account. The communication overheads were analyzed using the size of the exchanged message while This was used to denote the time needed for a "cryptographic one-way hash function" to compare the computational cost between LAKS-NVT and other compared schemes. The communication overheads and computational cost for LAKS-NVT are 3008 bits and 20 Th ≈ 0.01 seconds respectively. The LAKS-NVT scheme is designed to control security flaws by creating a provably secure and lightweight MAKA scheme for medical IoT that does not require a server verification table. It has been demonstrated to be secure against a variety of attacks, including impersonation, stolen SN, replay, and leaking verification table attacks. The LAKS-NVT may be enhanced with higher security and functionality to further suits the environment of practical medical IoT.

A study of the smart medical system (SMS) which involves a network of communication and sensor technology where the doctor does treatment to patient (online), involves cloud-based applications. The research aims to develop a cloud-based secure with efficient authentication framework (CSEF) and elliptic curve cryptography (ECC) for SMS (Kumari et al., 2020). The problem with SMS is that the communication is via a cloud server where the communication channel is insecure. This can cause the security issues such as patient and doctor unlinkability, anonymity, data confidentiality, and integrity. The use of wireless sensor networks in the medical system requires an authentication framework, which is more secure for the doctor, patient, related information, and other security elements, thus the attacker cannot access the data. This is where an efficient and secure mutual authentication framework with the presence of ECC and cloud is developed for smart medical systems (SMS) (Kumari et al., 2020). A study of the security analysis and the evaluation of CSEF where it can resist various security elements and attacks. This includes a man-in-the-middle attack where a method to avoid it is the cloud will verify the timestamp and message received by Healthcare Upload Phase and send the message to be verified by Healthcare Center. A hash value of parameters unique ID, the base point of additive ECC group,

and timestamp will be computed, then the message is sent to cloud to be verified. The attacker cannot enter this phase as the parameters are the crucial elements of the communication system with ECC (Kumari et al., 2020). For a strong replay attack, it involves the computation of hash value, decryption, encryption, different and session keys which requires the use of random numbers and current time value. ECC involves a one-way hash function that has high security in the network system thus, CSEF can avoid this attack (Kumari et al., 2020). An impersonation attack is where the attacker will try to impersonate a Healthcare Center, verify the timestamp, and guesses the unique ID. A hash value of parameters session keys, cloud, signature, and timestamp has a safe value thus, the attacker cannot do the impersonation (Kumari et al., 2020). A Stolen-verifier attack involves the methods of the hash value, encryption, dynamic pseudo-random, and decryption are used to prevent attacker accesses patient's dynamic pseudo-random and password (Kumari et al., 2020). A parallel session attack occurs when the attacker reuses an old message in the insecure channel and form a fresh request. The attacker will impersonate the participant and compute the session key. Components reposed of information in CSEF are required to form suitable keys, but this attack can be avoided as the attacker cannot obtain the session key. In the article, the computational cost of CSEF is 6TSign + 37TS + 56TH ≈ 2.3401 second. CSEF was compared with the other 6 frameworks. One of the other frameworks' computational costs is 10.85% less than CSEF computational framework but the framework is insecure against impersonation, off-line guessing, and fails in doctor unlinkability, patient anonymity, and session security. The other 5 frameworks have greater computational costs, compared to CSEF. In terms of communication cost, CSEF has 2976 bits which are lesser than the other frameworks. The comparative analysis showed the proposed framework has higher efficiency in terms of computational cost and communication cost. In this study, cloud services are significant in the future, thus cloud security becomes a concern. However, the communication between patient and doctor in SMS which involves cloud is not fully safe. This system includes various security challenges such as data confidentiality and integrity. This also includes the patient and doctor anonymity. In cloud-based SMS, the communication between entities is exposed to various attacks such as parallel session, man-in-the-middle, replay, stolen-verifier, and impersonation. In this article, a challenge was mentioned by a previous article that involves a medical system with the authentication framework and wireless sensor networks where it required an authentication framework that is efficient and secure so the attacker could not find the data of patient and doctor. Besides, various key agreement frameworks had been presented during the previous years, but the achievement is not adequate, and the construction's basic need had been disturbed by these protocols which led to elemental exclusion. The direction of research aims to develop an efficient and secure mutual authentication framework with the uses of ECC and cloud in SMS which can satisfy various security activities and secure against different attacks. ECC was used in the design of authentication protocol in SMS networks because of the complexity, thus it is difficult to break, and its security is stronger than the public key for other cryptosystems (Kumari et al., 2020).

In this study, WBAN consists of three communication components which are hub node (server collects information from sensor and relay to the system administrator), foreign network node, and sensor node. The WBAN platform must ensure that security between authorized communicated parties is met and confidentiality, un-traceability, integrity, and privacy. To advance the communication channel, the authors propose lightweight and secure anonymity preserving protocol for WBAN that focuses on the term of efficiency and security by implementing the strong hash function and session key agreement (Almuhaideb & Alqudaihi, 2020). In this paper, the author emphasized the second model of the authentication model which is centralized authentication. The mutual authentication was conducted through BAN logic methods. This study also discusses several attacks and techniques for mitigating them. Using the fortunate junction of keys and the ID credentials, the attacker may obtain device information stored in the SN or HN. In both protocols, the proposed scheme has a dynamic refresh function and protects the sensor identity and key session with random values. (Almuhaideb & Alqudaihi, 2020). For the sake of competency key length that enumerates the time complexity to the device parameters, adversary A has a low probability of launching a successful brute force attack. The proposed scheme uses the SHA - 2 lists of keys that has a key of 221 bits, so able to estimate the time complexity of the 2224 hash key. This makes the attacker cannot attempt an effective guessing0attack0on the system's hash function key or other parameters. The key size of the system's hash functions is adequate for the authentication process. (Almuhaideb & Alqudaihi, 2020). The proposed scheme is proved resistant to replay attacks due to the difficulty of the identity masking process. Therefore, adversary A unable to find out the sensor IDSN's true identity. To attack the system, they need to identify the IDSN, and they are unable to use the old identity created for the time being. (Almuhaideb & Alqudaihi, 2020). A collision attack happens when the attacker attempts a lot of possible combinations to crack the hash function to obtain the parameter values. The attacker is unable to perform this kind of attack as it is difficult to catch two separate messages with a similar value in the hash function. Since the proposed scheme implements the 224 bits, it is resistant to the collision attack as the hash function with the family key sizes of 22 4bits, 256 bits, and 38 4bits are categorized as a strong hash function that is unaffected by the collision attack. (Almuhaideb & Alqudaihi, 2020).

Asymmetric encryption is the most commonly used authentication scheme in modern technology, which WBAN devices cannot afford to use. In this study, the computation cost was 0.06 ms done based on the one-way hash function. Compared to other research, this research has a better computational cost with a reduction of 70% by implementing P-I and a reduction of 80% by implementing P-II. This study also has better security compared to other research due to the 224 bits the key size of the hash function used. Therefore, the same goes with the authentication overhead, this research is also better compared to the other research as it has the least communication cost and can withstand any security attacks. This is due to the 224 bits of the hash function, random number, updating foreign network identity, and masking sensor identity, and 32 bits for times and generation of session sequence numbers. (Almuhaideb & Alqudaihi, 2020). The authors stated that the mutual authentication scheme formal was proven by implementing the BAN logic. Based on the related work research, the discussion is more to the improvement of the communication channels, especially in WBAN to become more secure and able to withstand any possible attacks. Thus, the authors proposed several points, which are the session key update and secure key deletion that was not mentioned in the previous related work. (Almuhaideb & Alqudaihi, 2020). The future research will concentrate on scheme enhancement for WBAN networks using a lightweight key deletion scheme, as well as simulation using the Tamarin and Proverif methods. ***Eavesdropping Attack*** -The adversary can steal transmitted data from the link, which contains the ASN, S1, S2, t1, S3, S4, S5, S6, t2, IDAP parameters. Since r is random and new, the adversary cannot obtain the master key Ks from ASN. Second, the adversary cannot obtain n1 and n2 from S1 and S3 because the authentication parameters, BSN, are not available. Finally, the adversary is unable to obtain any parameter from S2 and S6 due to the one-way function h(.). ***Sensor Node Impersonation Attack*** - In this attack, it was assumed that the adversary corrupted an SN and obtained IDSN, ASN, BSN, and PKS from the memory. However, since all parameters are covered under the one-way function h(.), the essential parameters cannot be revealed from BSN and PKS at this stage. The r or User from ASN also cannot be obtained due to its randomness and freshness. Therefore, the new valid tuple cannot be created by the adversary. ***Replay Attack*** - When the SN sends information to the server, the timestamp t1 is generated, and S2 = h(IDSN, ASN, S1,t1,n1) is computed. As a result, the adversary is unable to acquire IDSN and n1, making it impossible to generate a new legitimate S2. As a result, the timestamp t1 cannot be changed since the server can verify t1's validity. When the server sends information to the SN, the process is equivalent to S2. In that case, creating a new valid S2 is difficult, and t2 cannot be modified. ***Sensor Node Capture Attack*** - The assumption had been made where the adversary can obtain as many SNs as possible, which also consists of several tuples. Fortunately, the ASN and BSN which contain the information of the master key are random and fresh and protected by one-way function h(.) respectively. Thus, the adversary cannot obtain any important parameters. ***Server Spoofing Attack*** - To perform a spoofing attack, the adversary needs the new valid tuple (S3, S4, S5, S6, t2). To create S3, they will need a User, which they cannot obtain. Thus, S3 cannot be created. The adversary also cannot obtain the parameters that are needed to create S4, S5, or S6. Therefore, the adversary cannot create a new valid tuple. ***Jamming/Desynchronization Attack*** - The adversary can interrupt contact at any time, resulting in the communication being unable to synchronize with the most recent updates. The device only needed to be restarted for a new round of authentication if the adversary blocked contact during steps A1 and A2. For steps A3 and A4, there are two tuples in the memory, (ASN+, X+, PKs+) and (ASN, X, PKs). The (ASN+, X+, PKs+) tuple is an updated authentication parameter while the other is the not updated parameter. When the SN restarted, the not updated parameter was still legit to be used to authenticate successfully. Thus, the jamming /desynchronization attack risk is avoided. For the computational cost, the proposed scheme uses the symbols of Th and Txor that represent the computing time. During the authentication phase, the SN carry out 5 hash functions operations and 5 XOR operations and the server carries out 7 hash function operation and 9 XOR operation. If a comparison is made between hash operation and XOR, the XOR operates for a very short time and is neglectable. The scheme is the solution for reducing the computational cost and with guaranteed security from all attacks. The proposed scheme has a lower risk of attack for the medical Internet of Things. The scheme can be applied not only for wideband area networks (WBAN) but also can be considered for other scenarios that require lightweight authentications scheme as well since it requires only hash function operations and XOR operations. In the future, the scheme can be more widely applicable to guaranteeing forward secrecy such as Internet of vehicles and mobile service computing without using asymmetric encryption.

Many researchers have worked on authentication in WBAN in which is both cryptographic and non-cryptographic. Cryptography has a high computation compared to the non-cryptographic which is based on physiological feature and channel characteristics. Therefore, it has simpler requirements and less computational overhead. Although these two schemes can achieve authentication in WBAN, the author chose the non-cryptographic method, the channel characteristic which is simpler and has less computation cost. However, most research works on channel characteristic-based authentication where it only considered one-way authentication and impersonate attack. In this study, the attacks considered are impersonation and eavesdropping attacks which are both passive and active attacks. To tackle these issues, mutual authentication schemes based on signal

propagation characteristic has been proposed. The signal propagation variations are between on-body and off-body channels to differentiate the legitimate and attacker devices (Ma et al., 2020). They also proposed a butterfly algorithm to generate the random number for the signal propagation variations. To conduct this mutual authentication experiment effectively, five volunteers have been invited under different scenarios for the indoor and outdoor environment (Ma et al., 2020). The current challenge is due to the limited resources and effect of the open nature of the corridor and the passer-by on the signal propagation and the walking scenario. In the future, the authors plan to investigate the authentication schemes that consider an attack from malicious devices that are placed on the user's body (on-body attackers), as well as the effect of the privileged insider, and random number leakage attacks on the performance.

3 Proposed Solution

The multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Network only use fingerprint identifier as biometric input. Assume the attacker has the access to the user's fingerprint, this is known as spoofing attacks where the attacker replicates the user's fingerprint and uses it for its benefit. In this contact, spoofing attacks occur when the attacker has successfully pretended to be the right person by using recreated fingerprint. In this report, we propose an innovation to this scheme by adding retinal-based biometric authentication to prevent spoofing attacks. Our retina is unique for each person and difficult to be recreated. This will enhance the application security by having retina and fingerprint authentication work side by side.

In the initial step, the user needs to install a health app on the phone and other BAN devices. Then the user is required to register an account. This account is mainly identifying the rightful user for all BAN devices connected in one single account. This account holds users' information such as private credentials, and biometric information such as retina and fingerprint. In the initial registration phase, the user will provide user biography information to the system. For the user security authorization, a user needs to provide image input of his/her retina images. Then, those images will be analyzed and extracted characteristics into data. These data will be stored in the system database. A similar process performs on fingerprint input. This process can be seen in figure 1 biometric registration process below. Upon complete registration, a user's BAN device with the registered account will automatically share information on the security authentication. A detailed explanation will be discussed further in this report.

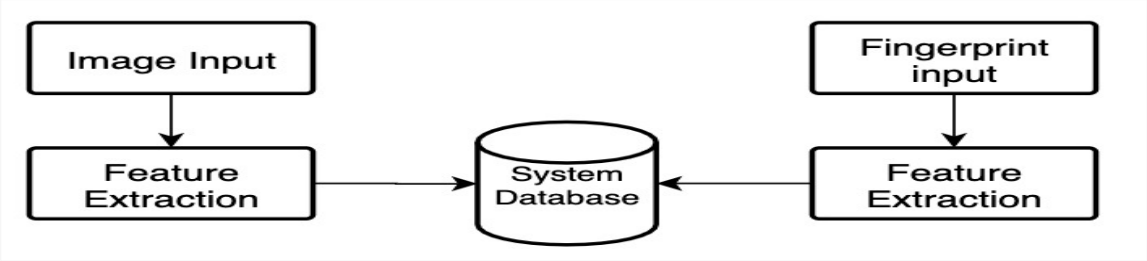

Figure 2: Biometric Registration process

To register their retina patterns and fingerprint, the users are required to log in their password through the application to make sure they are the owner of the registered biometric information. Then, the app will request for user's retina image for the scanning and extraction of features. Then the application will request fingerprint input for the same action on the retina image. All the extracted features will be stored in the system database to be retrieved for future authentication.

The feature extraction involves scanning the retinal images and fingerprint patterns. For the fingerprints, the system can directly extract from the fingerprint input by the user and store the pattern in the database. In extracting the retinal image, there are a few stages that undergo it. The first stage is the image retrieving itself. The image of the retina will be taken by using the fundus camera (through the hospital). The second stage is involving feature extraction based on the blood vessels that appeared in the user's retina (based on the images). Few features will be taken to confirm the owner identity of the retina.

- Branch Point- the features where the branch of a vessel started since the blood vessels are in a tree shape.
- End Point- the features that the vessels end in the retina. The endpoints of an individual retina are various and unique from the others.

- Crossover Point- the features where the blood vessels in the retina interest with each other and it is also a unique feature that the system will capture.
- The vessels in and around the Optic Disc- the blood vessels inside and around the optic is taken as a feature for the scanning purpose.

The last stage will be the testing part where the retinal image is tested and compared to the template features in the database. If the feature on the image satisfied the template feature, then the owner of the retinal will be authenticated successfully. This scanning part is the most secure way to authenticate since there is no way outsiders will make the copy of the retinal features although this improvement increases the computational time of the original scheme. This is due to the segmentation of features to extract the vessel pattern.

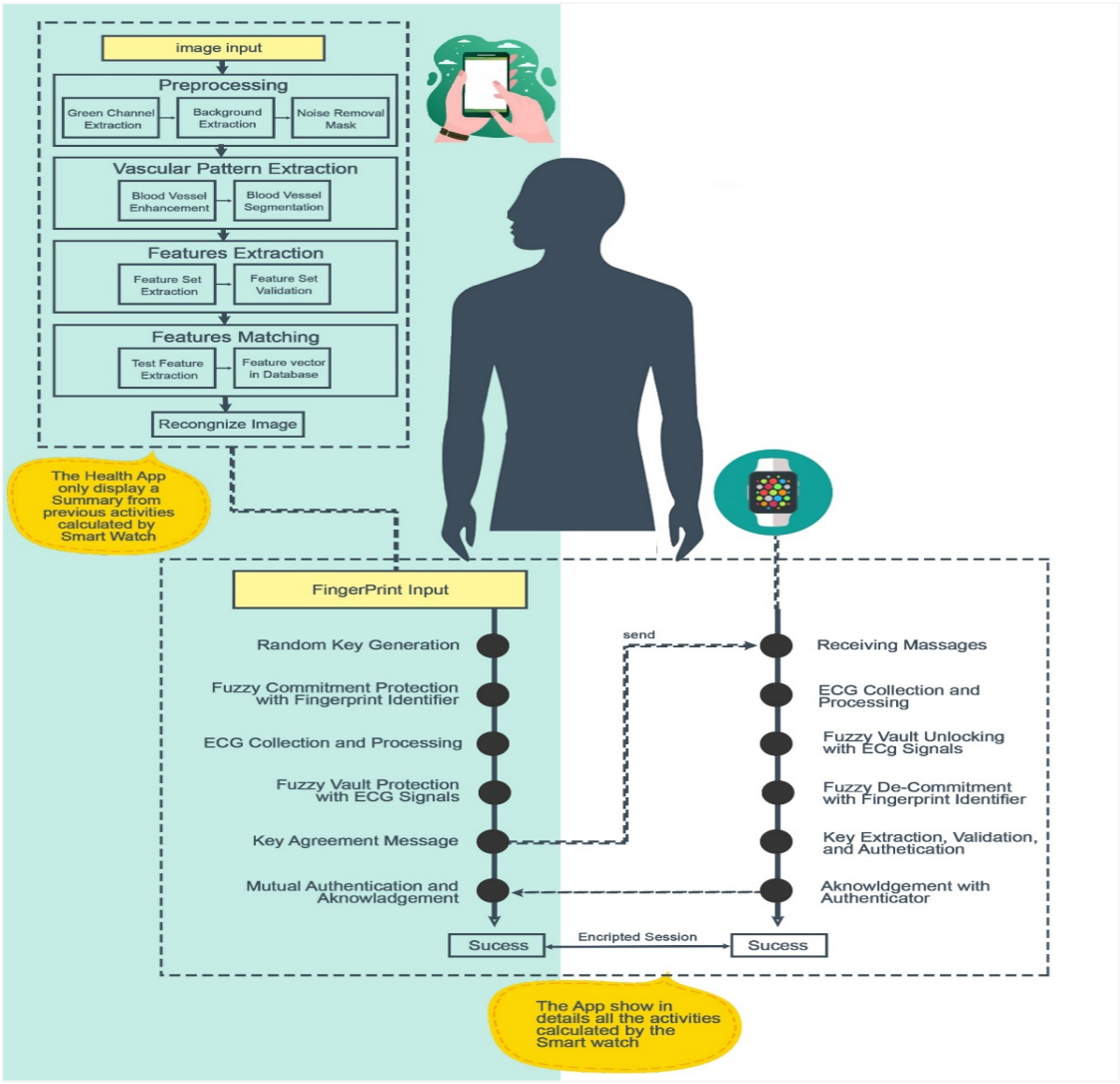

Figure 3: The improvement of the multi-Biometric and Physiological Signal-Based Key Agreement for BAN by adding retina capturing scheme

Figure 2 above shows the improved scheme of the multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Network by adding a retina capturing scheme. For a user to access their health information, the scheme imposed two-phase authentications. In the first phase, the system requires the user to scan their retina, and if successful the system will display a summary of the user's health. Then, the second phase is where the system requires the user to provide his/her fingerprint. If successful, a more detailed report for example real-time reading of heart rate will be displayed.

Phase 1: Retina input

Step 1 - A user scanned their eyes / provide an image input
Step 2 - Image processing. The image will undergo green channel extraction, background extraction, and noise removal mask.
Step 3 - Vascular Pattern Extraction. The system will enhance the blood vessel image, then continue to segmentize the blood vessel image.
Step 4 - Feature extraction is the process of bringing out the unique features based on steps 2 & step 3.
Step 5 - Feature Matching is the process of comparing the newly gathered data in step 4 with the data in the database.

If successful, the system will show the user's health summary. This summary will only show users vital information such as average heart rate, user walking distance, etc. To check further reports, the user needs to provide finger input which will be explained in detail in phase 2.

Phase 2: Fingerprint input

Step 1 - Same user in phase 1 scanned his/her fingerprint.
Step 2 - Random key will be generated
Step 3 - Fuzzy commitment protection with fingerprint identifier
Step 4 - ECG collection and processing
Step 5 - Fuzzy vault protection with ECG Signals
Step 6 - Key Agreement messages will be generated and sent to the targeted BAN device smartwatch.
Step 7 - The smartwatch receives the key agreement massages
Step 8 - Then the messages undergo ECG Collection processing
Step 9 - Fuzzy Vault Unlocking with ECG signals
Step 10 - Fuzzy De-commitment with fingerprint Identifier
Step 11 - Key extraction, validation, and authentication
Step 12 - If successful – the devices are mutually authenticating each other, and the encrypted session will start between the devices.

4 Security Analysis

In this section, we discussed the security analysis of our proposed that aims to add more security and robustness towards any possible security attacks. Besides, the size of retina biometric is quite small compared to other biometric characteristic (B. Mazumdar, 2018). These can lead to faster verification and identification process time. Depending on the implementation of ECG-based fuzzy vault and fingerprint-based fuzzy commitment only is not strong enough to secure the communication. Due to the modern world that is moving towards technology, the attacker has a wide range of options for attacking or disrupting communication. The fingerprint is easy and many ways to be duplicated, such as creating the artificial finger. In this paper, we will be discussing man-in-the-middle-attacks, node impersonation, and eavesdropping attacks.

MAN-IN-THE-MIDDLE ATTACKS - This happens when the stranger access and observe the traffic communication between two communicating devices, then carry out the attack such as stealing or fabricating the data. The proposed scheme proved able to resist man-in-the-middle-attacks. The key was protected by the implemented fuzzy commitment protection and fuzzy fault protection. Therefore, the attacker is unable to detect the key or create a similar key via the sniffing process and is unable to pass the authentication.

NODE IMPERSONATION - The proposed scheme is resistant against the impersonation attack in that it validates that the data was sent correctly by a legitimate user. Since our proposed scheme implemented the fingerprint-based fuzzy commitment, retina scan-based fuzzy commitment, and ECG-based fuzzy vault also because the authenticator and message exchanges supply mutual authentication. The attacker will face some challenges such as being time-consuming and requiring a lot of work to find the exact match of fingerprint and retina together with the features of the ECG.

EAVESDROPPING - The system is more resistant against eavesdropping attacks thanks to the implemented combination of ECG-based fuzzy vault, fingerprint-based fuzzy commitment, and retina-based fuzzy commitment. It has a variety combination of properties that makes the attacker unable to successfully, identify the perfect match of properties combination. During the process of exchanging session keys, the pairwise

session key must match between the sender and the receiver to enable successful authentication. The paired key will then encrypt the data, protecting it from eavesdropping attacks.

5 Complexity Analysis

In this section, we evaluate the proposed scheme complexity analysis by comparing it with the other 3 member's work (Almuhaideb & Alqudaihi, 2020; Park et al., 2020; Umar et al., 2020) from the previous assignment in terms of the authentication overhead and computational overhead. All other 3 works are also in the related field which is in the BAN field. However, the difference between the application and implementation of the BAN in the work will make some difference in the authentication overhead and computational overhead.

Authentication overhead (compare with other 3 members works)

In the improved scheme of the multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Network, the retinal scan was added as part of the authentication process. So, this has increased the authentication method and authentication overhead to authenticate the user. The length of identity or random number is assumed as 32 bits while 160 bits and 256 bits respectively for output size of hash function and block encryption/decryption. The authentication overhead is calculated to be around 1600 bits.

Table 1: Comparison of authentication overhead between the proposed scheme and other related work

Scheme	(Park et al., 2020)	(Almuhaideb & Alqudaihi, 2020)	(Umar et al., 2020)	Proposed scheme
Authentication overhead	1504 bits	432 bits (sensor node)	568 bits	1600 bits

Computational overhead (compare with other 3 members works)

Computational overhead is the time spent for the scheme to communicate in the network. Taking Reshan et al. (2019) as a reference as this proposed scheme is based on the computational overhead is evaluated with the strength of the security to withstand attacks such as man in the middle attack, node impersonation attack, and eavesdrop attack. Using the assumption in complexity analysis (i), the total communication overhead is expected to be around 2085 bits for the initial registration phase. The authentication overhead is relatively high compares to the other 2 works (Almuhaideb & Alqudaihi, 2020) and (Umar et al., 2020). However, despite having 3 authentication methods which are password, retinal scan, and fingerprint scan, and having more security due to its multiple authentication methods it still has a lower computational overhead compared to Park et al. (2020) Table 1 shows the comparison of computational overhead between the proposed scheme and other related work.

Table 2: Comparison of computational overhead between the proposed scheme and other related work

Scheme	(Park et al., 2020)	(Almuhaideb & Alqudaihi, 2020)	(Umar et al., 2020)	Proposed scheme
Authentication overhead	1504 bits	432 bits (sensor node)	568 bits	1600 bits

6 Conclusion

In this paper, we have proposed a new adding multifactor authentication scheme to the article MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks which is retina-based biometric authentication to prevent spoofing attacks. Since our retina is unique, it is difficult to be recreated. Plus, it is hard to be obtained from anywhere because it is difficult to be forge. This will enhance the application security by having retina and fingerprint authentication work side by side. This also helps to increase the level of security in the WBANs so that the attackers may not be able to access and falsify the data of the patients. Moreover, the security analysis characteristic demonstrates that the new purposed of authentication is robust to

spoofing attacks, Man-In-The-Middle attacks, Impersonation, and Eavesdropping Attacks. Last but not least, this improved authentication by offering simplicity, efficiency, and precision scheme.

Acknowledgements

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak to support this research work. This work is carried out as a short-term research-based class project.

References

Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2021). Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. *IEEE Internet of Things Journal*, 8(1), 65–84. https://doi.org/10.1109/jiot.2020.3020076

Adetunji, T. O., Zuva, T., & Appiah, M. (2018). A Framework of Bimodal Biometrics for E-assessment Authentication Systems. 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC). Published. https://doi.org/10.1109/iconic.2018.8601246

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1). https://doi.org/10.1002/ett.4150

Almuhaideb, A. M., & Alqudaihi, K. S. (2020). A Lightweight and Secure Anonymity Preserving Protocol for WBAN. *IEEE Access*, 8, 178183–178194. https://doi.org/10.1109/access.2020.3025733

Alzahrani, B. A., Irshad, A., Albeshri, A., Alsubhi, K., & Shafiq, M. (2020). An Improved Lightweight Authentication Protocol for Wireless Body Area Networks. *IEEE Access*, 8, 190855–190872. https://doi.org/10.1109/access.2020.3031484

B. Mazumdar, J. (2018a). RETINA BASED BIOMETRIC AUTHENTICATION SYSTEM: A REVIEW. *International Journal of Advanced Research in Computer Science*, 9(1), 711–718. https://doi.org/10.26483/ijarcs.v9i1.5322

B. Mazumdar, J. (2018b). RETINA BASED BIOMETRIC AUTHENTICATION SYSTEM: A REVIEW. *International Journal of Advanced Research in Computer Science*, 9(1), 711–718. https://doi.org/10.26483/ijarcs.v9i1.5322

Baba, E., Jilbab, A., & Hammouch, A. (2018). A health remote monitoring application based on wireless body area networks. 2018 International Conference on Intelligent Systems and Computer Vision (ISCV). Published. https://doi.org/10.1109/isacv.2018.8354042

Babu, P. S., & Sankar Panda, B. (2020). Light Weight Security and Authentication in Wireless Body Area Network(Wban). 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA). Published. https://doi.org/10.1109/iccsea49143.2020.9132854

Balan, K., F., L., S., A., A., -, Tarmizi, S., S., K., & Sallehudin, H. (2018). RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks. *International Journal of Advanced Computer Science and Applications*, 9(12). https://doi.org/10.14569/ijacsa.2018.091243

Dharanesh, C. M., Prasad, R., & Patil, C. M. (2017). Feature Extraction Classification for Personal Identification using Iris. 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). Published. https://doi.org/10.1109/ctceec.2017.8455060

Dharshini, S., & Subashini, M. M. (2017). An overview on wireless body area networks. 2017 Innovations in Power and Advanced Computing Technologies (i-PACT). Published. https://doi.org/10.1109/ipact.2017.8244985

Dildar, M. S., Khan, N., Abdullah, J. B., & Khan, A. S. (2017). Effective way to defend the hypervisor attacks in cloud computing. 2017 2nd International Conference on Anti-Cyber Crimes (ICACC). Published. https://doi.org/10.1109/anti-cybercrime.2017.7905282

Fatima, K., Nawaz, S., & Mehrban, S. (2019). Biometric Authentication in Health Care Sector: A Survey. 2019 International Conference on Innovative Computing (ICIC). Published. https://doi.org/10.1109/icic48496.2019.8966699

Harakannanavar, S. S., Renukamurthy, P. C., & Raja, K. B. (2019). Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends. *International Journal of Advanced Networking and Applications*, 10(4), 3958–3968. https://doi.org/10.35444/ijana.2019.10048

Jafer, E., Hussain, S., & Fernando, X. (2020). A Wireless Body Area Network for Remote Observation of Physiological Signals. IEEE Consumer Electronics Magazine, 9(2), 103–106. https://doi.org/10.1109/mce.2019.2953736

Ji, S., Gui, Z., Zhou, T., Yan, H., & Shen, J. (2018). An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services. *IEEE Access*, 6, 69603–69611. https://doi.org/10.1109/access.2018.2880898

Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. *IEEE Access*, 9, 87079–87093. https://doi.org/10.1109/access.2021.3088149

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors*, 19(22), 4954. https://doi.org/10.3390/s19224954

Khan, A. S., Javed, Y., Abdullah, J., & Zen, K. (2021). Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). *Journal of Ambient Intelligence and Humanized Computing*. Published. https://doi.org/10.1007/s12652-021-02968-6

Khan, A. S., Lenando, H., Abdullah, J., & Fisal, N. (2015). Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *Jurnal Teknologi*, 73(1). https://doi.org/10.11113/jt.v73.3258

Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending Malicious Script Attacks Using Machine Learning Classifiers. *Wireless Communications and Mobile Computing*, 2017, 1–9. https://doi.org/10.1155/2017/5360472

Kumari, A., Kumar, V., Abbasi, M. Y., Kumari, S., Chaudhary, P., & Chen, C. M. (2020). CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC. *IEEE Access*, 8, 107838–107852. https://doi.org/10.1109/access.2020.3001152

M, L., & V, K. (2019). A Survey on Iris Biometric and Recognition. *Journal of Advanced Research in Dynamical and Control Systems*, 11(11-SPECIAL ISSUE), 331–337. https://doi.org/10.5373/jardcs/v11sp11/20193039

Ma, Z., Yang, Y., Liu, X., Liu, Y., Ma, S., Ren, K., & Yao, C. (2020). EmIr-Auth: Eye Movement and Iris-Based Portable Remote Authentication for Smart Grid. *IEEE Transactions on Industrial Informatics*, 16(10), 6597–6606. https://doi.org/10.1109/tii.2019.2946047

Park, K., Noh, S., Lee, H., Das, A. K., Kim, M., Park, Y., & Wazid, M. (2020). LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things. *IEEE Access*, 8, 119387–119404. https://doi.org/10.1109/access.2020.3005592

Reshan, M. A., Liu, H., Hu, C., & Yu, J. (2019). MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks. *IEEE Access*, 7, 78484–78502. https://doi.org/10.1109/access.2019.2921822

Roy, S., Dutta, P., Bhowmik, A., Roy, B., Sourav, K., & Kumari, L. (2019). Identification of medical disorders in eye and biometric authentication analysis with iris retina scan using machine learning. *Biotechnology and Biological Sciences*, 29–33. https://doi.org/10.1201/9781003001614-5

Securing Cloud in Industrial IoT using Iris and Retina Scanner. (2019). *International Journal of Engineering and Advanced Technology*, 9(1), 6050–6054. https://doi.org/10.35940/ijeat.a1882.109119

Shokeen, S., & Parkash, D. (2019). A Systematic Review of Wireless Body Area Network. 2019 International Conference on Automation, Computational and Technology Management (ICACTM). Published. https://doi.org/10.1109/icactm.2019.8776847

Sridhar, M., Priya, N., & Muniyappan, A. (2020). Wireless Body Area Networks. Advances in Medical Technologies and Clinical Practice, 67–85. https://doi.org/10.4018/978-1-7998-1090-2.ch004

A Survey on Biometrics Security System. (2018). *International Journal of Recent Trends in Engineering and Research*, 4(3), 263–268. https://doi.org/10.23883/ijrter.2018.4127.p2pms

Umar, M., Wu, Z., & Liao, X. (2020). Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics. *IEEE Access*, 8, 66411–66422. https://doi.org/10.1109/access.2020.2985261

Wang, C., Zheng, W., Ji, S., Liu, Q., & Wang, A. (2018). Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks. *Wireless Communications and Mobile Computing*, 2018, 1–7. https://doi.org/10.1155/2018/4028196

Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., Khan, M. K., Karuppiah, M., & Baliyan, R. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Security and Communication Networks*, 9(16), 3527–3542. https://doi.org/10.1002/sec.1558