BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research

Volume 4 | Issue 3 | July 2022 | ISSN 2630-5151（Online）

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 4 Issue 3 • July 2022 • ISSN 2630-5151 (Online)

Journal of Computer Science Research

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 4 | Issue 3 | July 2022 | Page1-33
Journal of Computer Science Research

Contents

Articles

Review

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Certificateless Algorithm for Body Sensor Network and Remote Medical Server Units Authentication over Public Wireless Channels

Bahaa Hussein Taher[1] Muhammad Yasir[2] Abraham Isiaho[3] Judith N. Nyakanga[4*]

1. Huazhong University of Science & Technology, Wuhan, China
2. China University of Petroleum, Qingdao, China
3. Kaimosi Friends University College, Kaimosi, Kenya
4. Kenyatta National Hospital, Nairobi, Kenya

ARTICLE INFO

Article history
Received: 22 December 2021
Revised: 22 June 2022
Accepted: 5 July 2022
Published Online: 13 July 2022

Keywords:
Authentication
Body sensors
Security
Privacy
WBAN

ABSTRACT

Wireless sensor networks process and exchange mission-critical data relating to patients' health status. Obviously, any leakages of the sensed data can have serious consequences which can endanger the lives of patients. As such, there is need for strong security and privacy protection of the data in storage as well as the data in transit. Over the recent past, researchers have developed numerous security protocols based on digital signatures, advanced encryption standard, digital certificates and elliptic curve cryptography among other approaches. However, previous studies have shown the existence of many security and privacy gaps that can be exploited by attackers to cause some harm in these networks. In addition, some techniques such as digital certificates have high storage and computation complexities occasioned by certificate and public key management issues. In this paper, a certificateless algorithm is developed for authenticating the body sensors and remote medical server units. Security analysis has shown that it offers data privacy, secure session key agreement, untraceability and anonymity. It can also withstand typical wireless sensor networks attacks such as impersonation, packet replay and man-in-the-middle. On the other hand, it is demonstrated to have the least execution time and bandwidth requirements.

1. Introduction

Wireless Body Area Networks (WBAN) comprise of interconnected nano-sensors that are deployed to collect biomedical data from the patients. Thereafter, the sensed data are forwarded to the remote medical servers for analysis and appropriate action [1]. Some of the collected data may include body temperatures, blood pressure and sugar levels [2]. As described by Farooq, S. et al. [3], WBAN is a form of Wireless Sensor Network (WSN). The sensors in WBAN may be placed on the skin, in the vicinity of the

*Corresponding Author:
Judith N. Nyakanga,
Kenyatta National Hospital, Nairobi, Kenya;
Email: nyakinajudith@gmail.com

DOI: https://doi.org/10.30564/jcsr.v4i3.4258

patient or implanted in the patient's body [4]. During the transmissions from the patient side towards the hospital medical servers, wireless public channels [5] are utilized. This two-way communication allows remote monitoring and surveillance of the patients, elderly as well as the disabled population. In so doing, this technology boosts efficiency and safety, as well the reduction of associated healthcare costs. There is also some element of automated control of important healthcare parameters as well as movements, which are then forwarded to hospital servers for appropriate action [6]. In addition, this technology enhances pervasiveness, query handling as well as emergency healthcare services in a multi-hop topology. Moreover, timely intervention may serve to improve the patient's quality of life [7]. The increased demand for WBAN has led to the development of IEEE 802.15.6 communication standard. This allows for seamless connections among low power sensor devices and in so doing, expands the range of applications.

In spite of the many benefits that accrue from the deployment of WBANs, many security and privacy issues surround the deployment and usage of these networks. This is because of the sensitive and private nature of the data transmitted in open wireless channels. As such, any successful data compromise violates patient privacy, can inadvertently lead to misdiagnosis and erroneous treatment, as well as the endangering of patient life [7]. As discussed by Nyangaresi, V.O. et al. [8], WBAN is a special type of WSN and therefore inherits all security risks in these networks. The various attacks that can be launched in WBAN can be classified as internal, confidentiality breaches, external, active and passive [9]. Another significant requirement in WBAN is trust building among the participants such as medical staff, patients and healthcare providers. As such, high levels of trust are one of the critical success factors that serve to boost reliable data exchange among the communicating entities [4].

Based on the discussions above, it is evident that attackers can leak, misuse and corrupt the mission-critical WBAN data. This may lead to wrong medication, job loss or even humiliation [10]. Therefore, WBANs have serious privacy, security and trust threats that may hinder their full potential in the healthcare industry. As such, the secure exchange of medical data in the face of active and passive attacks is necessary but quite challenging. All these issues point to the necessity of protecting WBANs against unauthorized access as well as data compromise. In light of this, proper authentication among all the communicating entities serves as the first step towards security and privacy protection [11]. Any weak authentication facilitates illegal access to healthcare data including malicious modifications, deletion and insertion of bogus data. As explained above, all this can have devastating effects on the side of the patients. Although many authentication protocols [12] have been developed to offer security and privacy in communication networks, their deployment in WBANs is problematic due to the resource constrained nature of body sensors [13,14]. These limitations manifest themselves in form of computation abilities, battery power and memory. There is therefore need to encipher all the data before its transmission over insecure public channels. Since most of the body sensors may be implanted in the patient body, battery replacement presents some challenges. As such, it is critical for the authentication schemes to be energy-efficient. Therefore, this paper makes the following contributions:

- Temporary identifiers are deployed during information exchange to offer anonymity and prevent traceability attacks.
- Random numbers are incorporated in the transmitted data to offer freshness checks and hence protect against packet replays.
- Lightweight bitwise XOR and one-way hashing operations are utilized to enhance the efficiency of the developed algorithm. As such, it is shown that our algorithm has the least execution time and bandwidth requirements.
- Informal security analysis is carried out, which demonstrate that this algorithm can withstand numerous WBAN attacks.

The rest of this paper is organized as follows: Section 2 presents related work, while Section 3 provides a description of the proposed algorithm. On the other hand, Section 4 presents security analysis while Section 5 discusses the performance evaluation of this algorithm. Towards the end of this paper, Section 6 concludes the paper and gives future research directions.

2. Related Work

Many schemes have been put forward to offer protection to patient data exchanged over WBANs. For instance, to build trust among the WBAN participants, numerous blockchain-based protocols have been presented [15-18]. However, blockchain technology is computationally and memory intensive [19]. In addition, the scheme presented by Cheng, X. et al. [16] has not been evaluated in terms of communication costs and attack models. To provide authentication between two nodes and reduce storage costs, a security scheme is developed by Liu, X. et al. [20]. However, this scheme is not evaluated in terms of privacy and other attack scenarios. On the other hand, symmetric key based protocols have been introduced by Sammoud, A. et al. [21] and Renuka, K. et al. [22]. However, the scheme

developed by Renuka, K. et al. [22] has high computation and execution time at the server side. Another secure and privacy preserving certificateless protocol is presented by Mwitende, G. et al. [23]. Unfortunately, this scheme has high computation overheads at the client-side. In addition, its analysis against security attacks is missing. To address these issues, an anonymous authentication scheme is introduced by Nyangaresi, V.O. et al. [24]. To offer mutual authentication, a three-factor scheme is presented by Sahoo, S.S. et al. [25]. Although this protocol has low communication and computation overheads, it is never evaluated against common security features such as non-repudiation, untraceability and unlinkability. Similarly, numerous security attacks analyses are missing in schemes developed by Pirbhulal, S. [26] and Peter, S. et al. [27]. To prevent traceability attacks against the user, a robust authentication scheme is presented by Wu, F. et al. [28]. However, significant security attacks analyses are not addressed in this approach. Similarly, resilience against eavesdropping, modifications, packet replays and Man-in-the-Middle (MitM) is not investigated in the protocol presented by Liu, J. et al. [29].

To offer secure data communication in WBAN, a digital signature based scheme is presented by Anwar, M. et al. [30]. The asymmetric key generation deployed here requires communicating entities to have pairs of private and public keys. This renders the algorithm quite inefficient and sophisticated [31]. To address this inefficiency challenge, an energy-efficient authentication protocol is presented by Chang, C.C. et al. [32]. Unfortunately, this protocol is not analyzed against various attack models. To provide conditional privacy, an authentication protocol is introduced by Tan and Chung [33]. However, this technique is vulnerable to Denial of Service (DoS) and impersonation attacks. On the other hand, anonymity preserving scheme that is capable of tracing malicious users is developed by Jegadeesan, S. et al. [34]. Unfortunately, this scheme is not evaluated against eavesdropping, MitM, impersonation and modification attacks. As explained by Shim, K.A. [35], impersonation and failure to offer non-repudiation and mutual authentication are key challenges for the scheme developed by Xiong and Qin [36]. To offer mutual authentication between a client and an access point, a scheme based on Elliptic Curve Cryptography (ECC) and bilinear pairing operations is introduced by Zhao, Z. [37]. However, this scheme is computationally intensive due to the deployed pairing operations [38]. To prevent MitM, impersonation, session hijacking and DoS attacks, an authentication approach is introduced by Zebboudj, S. et al. [39]. However, this protocol has not been analytically evaluated. On the other hand, an ECC based user authentication scheme is developed by Challa, S. et al. [40]. However, this protocol cannot withstand impersonation attacks.

Based on user biometrics, a retina-based security scheme is presented by Ullah, M.G. et al. [41]. Unfortunately, the authors fail to offer evaluation against security attacks. To address this challenge, mutual authentication protocols are introduced by Jiang, Q. et al. [42] and Abina, P. et al. [43]. However, the scheme developed by Jiang, Q. et al. [42] cannot withstand stolen verifier and packet replay attacks. On its part, the protocol by Abina, P. et al. [43] is susceptible to node compromise attacks. Similarly, the scheme presented by Zhou, L. et al. [44] is susceptible to packet replays, MitM, privileged-insider and impersonation attacks. To curb these security challenges, a certificate based authentication scheme is presented by Nyangaresi, V.O. et al. [45], while a user authentication protocol is presented by Farash, M.S. et al. [46]. However, vulnerabilities against offline guessing and impersonation attacks are serious issues in the scheme developed by Farash, M.S. et al. [46]. Similarly, the scheme introduced by Sharma, G. et al. [47] is susceptible to impersonation attacks. Anonymity is another important requirement that must be fulfilled in WBAN authentication protocols. As such, an anonymous authentication scheme is introduced by Javali, C. et al. [48]. Unfortunately, this scheme has very high computation costs. To solve this performance issue, a lightweight authentication protocol is developed by Wazid, M. et al. [49]. In addition, a device pairing scheme for shared key generation is developed by Javali, C. et al. [50]. However, the authors fail to evaluate this protocol against forgery, packet replays and DoS attacks. To address these security issues, an authentication technique is presented by Zhang, W. et al. [51]. This scheme is shown to be robust against tampering, impersonation and replay attacks. However, its design fails to consider inlinkability and anonymity.

The Physically Unclonable Function (PUF) presents another significant technology in the prevention of physical and side-channeling attacks. For instance, numerous PUF based schemes have been presented by different researchers [52-55]. However, PUF based schemes have stability issues. On the other hand, signature based schemes have also been developed to prevent non-repudiations. For instance, a lightweight distributed model based on signatures is introduced by Alaparthy and Morgera [56], while an energy-efficient scheme for key agreement and authentication is developed by Iqbal, J. et al. [57]. Unfortunately, many security attacks cannot be prevented in this protocol [57]. An authentication scheme for wearable sensors has been developed by Li, X. et al. [58]. However, this protocol lacks unlinkability and forward key secrecy [59]. To address these issues, an improved security and priva-

cy-preserving technique is presented by Khan, H. et al. [60]. Similarly, an Advanced Encryption Standard (AES) based scheme that can offer strong forward key secrecy is introduced by He and Zeadally [61]. However, these schemes have key escrow problems in that the central node is required to store master keys as well as security parameters for all other nodes [62]. In addition, the protocol developed by He and Zeadally [61] cannot provide non-repudiation and protection against known secret key attacks. Although impersonation attacks are prevented in the protocol developed by He, D. et al. [63], this scheme cannot provide resilience against key escrow, non-repudiation, linkability and known secret key attacks.

To offer robust security protection, intrusion detection systems [64] and bilinear pairing based schemes developed by Wang and Zhang [65] and Xiong, H. [66] have been presented. Although this scheme by Wang and Zhang [65] offers anonymity, it fails to take into consideration storage overheads. In addition, both schemes have high computation complexities due to the bilinear pairings [67]. Smart cards present another important technique for WBAN authentication. In this regard, an efficient and privacy preserving scheme is developed by Chia-Hui and Yu-Fang [68]. However, this protocol cannot withstand stolen smart card, forgery, packet replays and offline guessing attacks. Group authentication-based protocols have also been developed to deal with security and privacy issues in WBANs. For instance, a group authentication scheme for sensor and personal digital assistant authentication is presented by Shen et al. [69]. However, this scheme cannot provide protection against packet replays, linkability, impersonation, MitM and packet replays. In addition, this scheme is vulnerable when some group members turn out to be malicious [70]. Although digital certificate based schemes can help address this challenge, certificate and public key management presents high complexity for body sensors.

3. The Proposed Algorithm

The medical staff, Trusted Authority (TA), Mobile Device (MD) and the body sensor (BS) are the major components in the proposed algorithm. As shown in Figure 1, the link between the body sensors and the medical staff's MD is an open wireless channel.

Here, the medical staff deploys the MD to access the body sensor data. On the other hand, the TA registers and issues the required security parameters to the body sensors and MDs to help them authenticate each other. Table 1 gives the notations used in this paper.

In term of execution, this algorithm comprises of four main phases, which include medical staff registration, sensor registration, authentication and session key agreement. These phases are explained in greater details in the sub-sections that follow.

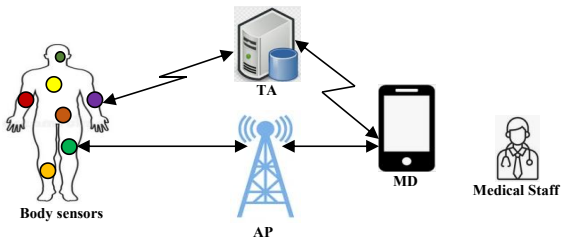

Figure 1. Network Model

Table 1. Notations

Symbol	Description
ID_M	Mobile device unique identity
ID_S	Body sensor unique identity
R_i	Random number *i*
TID_M	Mobile device temporary identifier
TID_A	Trusted authority temporary identifier
TID_B	Body sensor temporary identifier
SKi	Session keys
h(.)	Hashing operation
||	Concatenation operation
$\oplus$	XOR operation

3.1 Medical Staff Registration

In this phase, any smart mobile device is deployed by the staff to register with the trusted authority before any access to patient information residing in the body sensors is granted. This is a four-step as shown below.

Step 1: The medical staff *Ui* chooses and inputs unique identity *IDM* and password *PWi* to the MD. Next, the MD constructs registration request message *RM1 = {IDM, PWi }* that is forwarded to the TA over some secure channels.

Step 2: Upon receiving *RM1* from the user's MD, the TA stores its contents in its database. Afterwards, it generates random number *R1* that it uses to derive security parameter $A1 = (IDM \oplus R1) \oplus PWi$.

Step 3: The TA generates *TIDM* as the user's mobile device temporary identity. Next, it computes parameter $A2 = R1 \oplus IDM$. Thereafter, it stores {*R1, TIDM*} in its database before sending parameter *A1* back to the user's MD.

Step 4: After getting *A1* from the TA, the MD computes nonce $R1^* = (A1 \oplus PWi) \oplus IDM$ and temporary identity $TIDM = R1^* \oplus IDM$. This is followed by the stor-

ing of parameter set *{R1*, TIDM}* in the MD's memory. Finally, the MD derives parameter $A3 = (PWi||R1^*) \oplus TIDM$ that it stores in its memory.

3.2 Sensor Registration

In this phase, the sensor placed in the vicinity of the patient, implanted in the patient body or on the patient's skin need to register to the TA before forwarding the collected data to the medical staff. This is a three-step procedure as elaborated below.

Step 1: The body sensor extracts its identity *IDS* from memory. Afterwards, it generates random number *R2*. Next, it generates registration request message $RM2 = (IDS||R2)$ that it forwards to the TA over private channels.

Step 2: On getting message *RM2* from the body sensor, the TA extracts and stores parameter set *{IDS , R2}* in its database. Next, the TA generates random number *R3* that it utilizes to derive parameter $B_1 = (IDS \oplus R3) \oplus R1$ and its temporary identity $TIDA = R3 \oplus IDS$. Thereafter, the TA stores parameter set *{R3, TIDA}* in its database. Lastly, the TA forwards authentication message *RM3 = {B1}* over to the body sensor through some private channels.

Step 3: After getting message *RM3* from the TA, the body sensor computes $R3^* = (B1 \oplus R2) \oplus IDS$. Finally, it derives its temporary identity as $TIDB = R3^* \oplus IDS$ before storing parameter set $\{R_2, R_3, TID_A\}$.

3.3 Authentication and Key Agreement Phase

In this phase, the medical staff and the body sensor execute mutual verification of each other before any access to the sensed data is permitted. This is a nine-step process as described below.

Step 1: The medical staff inputs password *PWi* to the MD after which it derives parameter $B2 = h(PWi||R1) \oplus TIDM$. Next, the MD validates *B2* against *A3* that is stored in its memory. Provided that these two values are unequal, the session is terminated. Otherwise, the MD generates random number *R4* which it uses to derive parameters $B3 = R4 \oplus PWi$ and $C1 = h(R1||PWi)$. Finally, it composes authentication message *AM1 = {B3, TIDM, C1, TIDA}* that is sent to the TA as shown in Figure 2.

Step 2: On receiving message *AM1* from the MD, the TA retrieves *R4* from *B3*. Next, the freshness of random number *R4* is verified. Here, the session is terminated if *R4* fails the freshness check. Otherwise, the TA extracts *TIDM* and *TIDA* from its database and compares these values against the ones received in message *AM1*. Basically, the session is terminated when there is no match. Otherwise, the algorithm shifts to step 3 below.

Step 3: The TA derives parameter $C1^* = h(R1||PWi)$. It then retrieves *C1* from its database and compares it against *C1**. If there is a mismatch, the session is terminated. Otherwise, the TA has successfully authenticated the user's MD. Next, the TA generates random number *R5* that it uses to compute $C2 = (TIDA \oplus R5)$. Next, it computes $C3 = h(R2||R3)$ and session key *SK1* that it masks in parameter $\phi = (SK1 \oplus R2) \oplus R5$. Thereafter, it derives and stores parameter $D1 = (R3 \oplus R2)$ in its database. Finally, it constructs authentication message *AM2 = {C2, C3, TIDM, ϕ, D1}* that it sends to the body sensor.

Step 4: After getting message *AM2*, the BS extracts *R5* from *C2* and validates its freshness. Here, the session is aborted if random number *R5* fails the freshness check. Otherwise, the BS derives parameter $D2 = h(R2||R3)$ followed by its verification against *C3*. Essentially, the session is terminated if the two values do not match. Otherwise, the BS has successfully authenticated the TA.

Step 5: The BS extracts *SK1* from ϕ as $SK1 = (\phi \oplus R5) \oplus R2$ followed by the generation of random number *R6* that is employed to compute security parameters $D3 = (R6 \oplus TIDA)$, $E1 = h(R3^*||R2||SK1)$ and $E2 = (R3 \oplus R2)$. Next, it retrieves *R3* from *D1* as $R3 = (D1 \oplus R2)$. It also computes new temporary identity $TIDB^* = R3^* \oplus IDS$ before storing parameter set *{R2, R3, TIDB*}* in its memory. Lastly, it composes authentication message *AM3 = {D3, E1, E2}* and forwards it to the TA.

Step 6: On receiving message *AM3* from the BS, the TA extracts random number *R6* from *D3* as $R6 = (D3 \oplus TIDA)$ and validates its freshness. Provided that this message passes the freshness check, the TA derives $E1^* = h(R3||R2||SK1)$. Next, parameter *E1** is validated against *E1* such that the BS is considered successfully authenticated by TA if this verification is successful. This also confirms the correctness of the derived session key *SK1*.

Step 7: The TA retrieves *R2* from *E2* as $R2 = (E2 \oplus R3)$ and derives $TIDB^* = R3 \oplus IDS$. Next, it stores parameter set *{R3, TIDB*}* in its database. Next, it generates random number *R7* that it deploys to compute $E3 = IDM \oplus R7$. This is followed by the computation of MD's session key $SK2 = (\phi \oplus PWi) \oplus R7$.

It then generates random number *R8* before computing $F1 = h(IDM||PWi||SK2||R7)$ and $F2 = (R8 \oplus PWi)$. Next, it derives temporary identifier $TIDMNew = R8 \oplus IDM$. Finally, it stores parameter set *{R8, TIDMNew}* in its database and sends authentication message *AM4 = {E3, SK2, F1, F2}* towards the MD.

Step 8: The MD retrieves random number *R7* as $R7 = E3 \oplus IDM$ and validates its freshness. Provided that it passes this test, the MD derives session key $SK3 = (SK2 \oplus R7) \oplus PWi$ and parameter $F3 = h(IDM||P-$

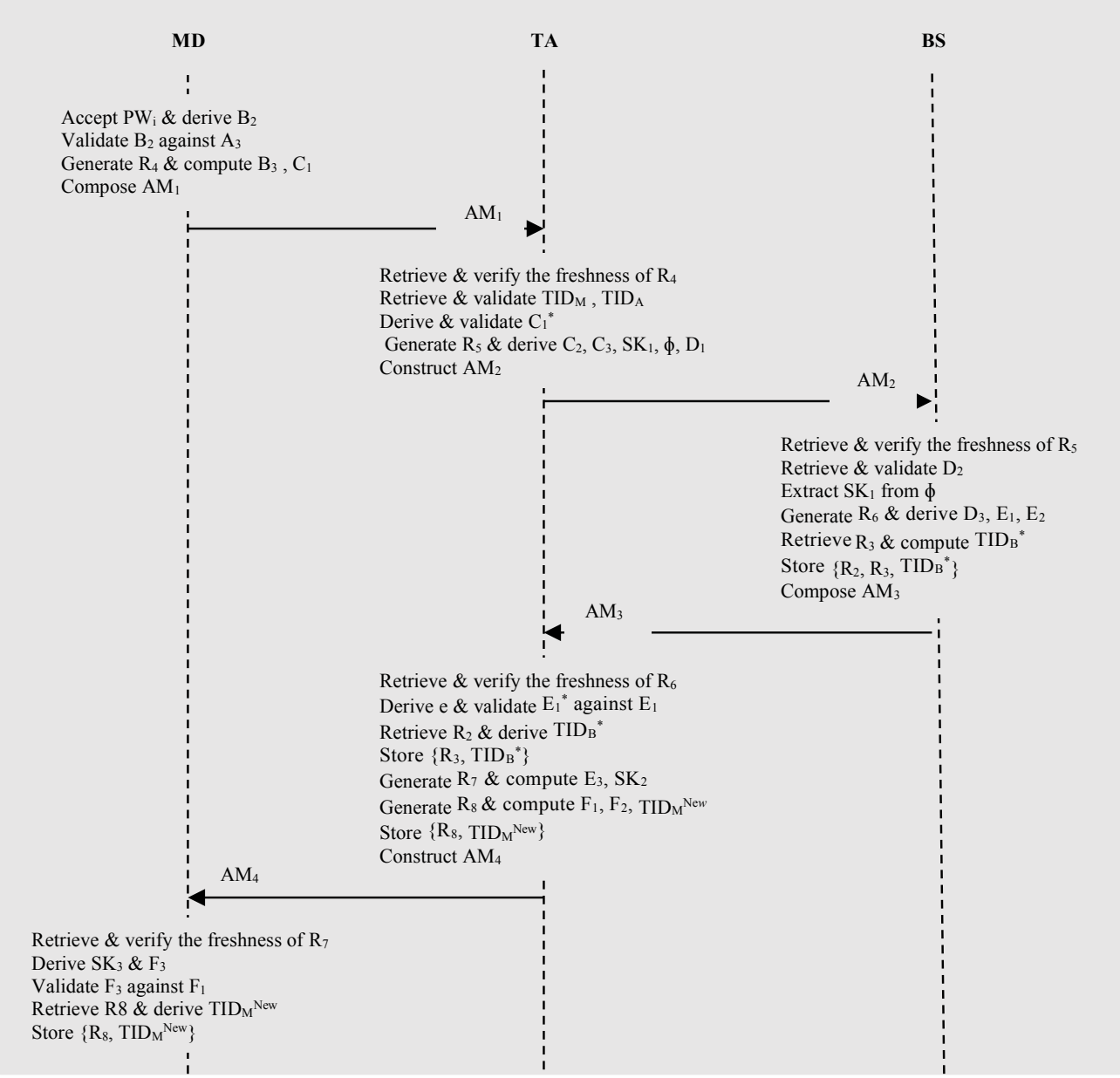

Figure 2. Authentication and Key Agreement Message Flows

Wi||SK3||R7). Thereafter, a comparison is made between *F3* and *F1* such that any match implies successful authentication between the MD and the TA. In addition, it indicates that the session key derived by the MD is valid.

Step 9: The MD retrieves *R8* from *F2* as *R8= (F2⊕PWi)* and derives new temporary identity *TIDMNew = R8⊕IDM*. Finally, it stores parameter set *{R8, TIDMNew}* in its memory.

4. Security Analysis

In this section, informal security analysis is executed to show the robustness of the proposed algorithm against conventional WBAN attacks vectors. To accomplish this, the following theorems are formulated and proofed.

Theorem 1: Data privacy is assured in this algorithm

Proof: Suppose that the adversary captures messages *AM1 = {B3, TIDM, C1, TIDA}*, *AM2 = {C2, C3, TIDM, ϕ, D1}*, *AM3 = {D3, E1, E2}* and *AM4 = {E3, SK2, F1, F2}* that are exchanged during the authentication and session key agreement phase. Here, *B3 = R4⊕PWi*, *TIDM = R8⊕IDM*, *C1 = h (R1||PWi)*, *TIDA = R3⊕IDS*, *D3 = (R6⊕TIDA)*, *E1 = h (R3*||R2||SK1)*, *E2 = (R3⊕R2)*, *E3 = IDM⊕R7*, *SK2 = (ϕ⊕PWi)⊕R7*, *F1 = h (IDM||PWi||SK2||R7)* and *F2 = (R8⊕PWi)*. Clearly, the attacker is unable to obtain real information concerning the communicating entities because of the bitwise XOR

and the collision-resistant one-way hashing operations. As such, an attacker is unable to read the contents of the exchanged messages.

Theorem 2: This algorithm can withstand packet replay attacks

Proof: The assumption made in this attack is that messages *R4*, TIDM, C1* and *TIDA* have been captured by an adversary. Later on, an attempt is made to replay these messages to unsuspecting entities. Here, $R4 = B3 \oplus PWi$, $TIDM = R8 \oplus IDM$, $B3 = R4 \oplus PWi$, $C1 = h(R1||PWi)$ and $TIDA = R3 \oplus IDS$. Evidently, all these messages contain random numbers whose freshness is checked at the receiver end. Upon the failure of the freshness checks, the session is terminated. Any modification of these random numbers will fail due to their masking in other parameters.

Theorem 3: This algorithm offers secure session key agreement

Proof: To secure the exchanged messages, the body sensor and the MD negotiate a session key to encipher all the exchanged messages. During this process, the trusted authority acts as an intermediary by providing the necessary keying parameters. After successful mutual authentication, the TA masks the body sensor session key *SK1* in security parameter $\phi = (SK1 \oplus R2) \oplus R5$ before transmitting it to the BS in message *AM2*. Similarly, the TA masks MD session key $SK2 = (\phi \oplus PWi) \oplus R7$ in parameter $F1 = h(IDM||PWi||SK2||R7)$ before forwarding it to the MD in message *AM4*. Thereafter, the MD and the body sensor deploy these session keys to encrypt messages before coupling them to the public communication channels. Suppose that an attacker has captured both messages *AM2* and *AM4*. However, without knowledge of *R2, R5, PWi* and *R7*, the attacker cannot retrieve these session keys from the captured messages.

Theorem 4: Man-in-the-middle attacks are thwarted in this scheme

Proof: Suppose that an attacker has captured message *AM1 = {B3, TIDM, C1, TIDA}*. Next, an attempt is made to modify it so as to fool other communicating entities. Here, $B3 = R4 \oplus PWi$, $TIDM = R8 \oplus IDM$, $C1 = h(R1||PWi)$ and $TIDA = R3 \oplus IDS$. However, the one-way hashing and bitwise XOR operations on these parameters imply that they cannot be easily altered. Similarly, messages *AM2*, *AM3* and *AM4* cannot be modified by an attacker.

Theorem 5: This scheme upholds untraceability and anonymity

Proof: The aim of the adversary here is to extract the identities of the communicating entities from the captured messages. Suppose that messages *AM1, AM2*, *AM3* and *AM4* have been successfully obtained by the attacker. Here, *AM1 = {B3, TIDM, C1, TIDA}*, *AM2 = {C2, C3, TIDM, ϕ, D1}*, *AM3 = {D3, E1, E2}* and *AM4 = {E3, SK2, F1, F2}*. Clearly, real identity information of the communicating entities is never sent in plaintext in all these messages. Instead, only temporary identities such as *TIDM* and *TIDA* are exchanged in these messages. In addition, these temporary identities are refreshed after every successful authentication process, such as in $TIDMNew = R8 \oplus IDM$. Therefore, the communication process in this algorithm is completely anonymous.

Theorem 6: Impersonation attacks are prevented in this scheme

Proof: Suppose that an attacker has captured message *AM2 = {C2, C3, TIDM, ϕ, D1}*. Thereafter, an attempt is made to extract body sensor and user secret information to impersonate these two entities. However, $C2 = (TIDA \oplus R5)$, $C3 = h(R2||R3)$, $TIDM = R8 \oplus IDM$, $\phi = (SK1 \oplus R2) \oplus R5$ and $D1 = (R3 \oplus R2)$ do not contain these secrets in plaintext. The utilization of one-way hashing and bitwise XOR operations impede any attempt to discern these secrets from the exchanged messages. The implication is that an attacker lacks real identities or secrets of the communicating entities. Therefore, any impersonation attack using message *AM2* or any other message will fail.

5. Performance Evaluation

In this section, we utilize execution time and bandwidth requirements to evaluate the performance of this algorithm.

5.1 Execution Time

The cryptographic operations carried out during the authentication and key agreement phase include three hashing operations (T_H) at the MD, $3T_H$ operations at the TA and $2T_H$ operations at the BS. The bitwise XOR operations are ignored since they have extremely low execution time compared with other cryptographic primitives. Therefore, the total execution time is $8T_H$ operations. Using the values by Srinivas, J. et al. [71], a single T_H operation takes 0.32 ms. As such, the total execution time for this algorithm is 2.56 ms. Table 2 presents the comparison of this execution time with other schemes.

Table 2. Execution time comparisons

Scheme	Operations	Time (ms)
[41]	$12T_H$	3.84
[44]	$36T_H$	11.52
[46]	$32T_H$	10.24
[47]	$23T_H$	7.36
[49]	$32T_H$	10.24
Proposed	$8T_H$	2.56

As shown in Figure 3, the scheme developed by Zhou, L. et al. [44] has the highest execution time, followed by the schemes developed by Farash, M.S. et al. [46] and Wazid, M. et al. [49] respectively. On the other hand, the protocol presented by Sharma, G. et al. [47] has the third highest execution time, while the scheme developed by Ullah, M.G. et al. [41] has the fourth highest execution time.

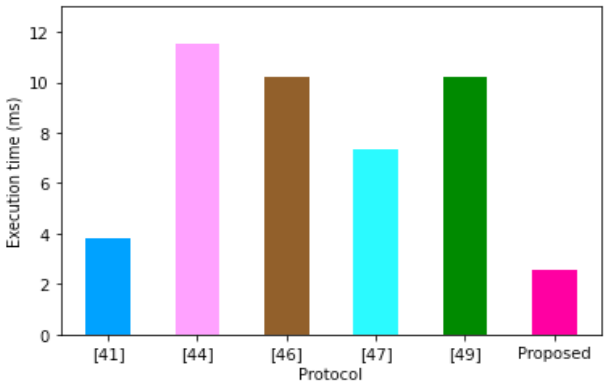

Figure 3. Execution time comparisons

It is evident that the proposed algorithm has the shortest execution time of only 2.56 ms. As such, it is the most ideal for deployment in computation power limited body sensors.

5.2 Bandwidth Requirements

To compute the number of exchanged bits, the four messages exchanged during the authentication and key agreement phase are considered. These messages include *AM1 = {B3, TIDM, C1, TIDA}*, *AM2 = {C2, C3, TIDM, ϕ, D1}*, *AM3 = {D3, E1, E2}* and *AM4 = {E3, SK2, F1, F2}*. Using the values by Srinivas, J. et al. [71], hashing output and ral identities are 160 bits long. On the other hand, random numbers and timestamps are 128 bits and 32 bits respectively. As such, the total size of these four messages is 2048 bits. Table 3 presents the bandwidth comparisons with other algorithms.

Table 3. Bandwidth comparisons

Scheme	Size (ms)
[41]	2528
[44]	3850
[46]	2752
[47]	2912
[49]	2400
Proposed	2048

Based on the plots in Figure 4, the scheme presented by Zhou, L. et al. [44] has the highest bandwidth consumption. This is followed by the approaches developed by Sharma, G. et al. [47], Farash, M.S. et al. [46], Ullah, M.G. et al. [41], Wazid, M. et al. [49] and the proposed algorithm respectively.

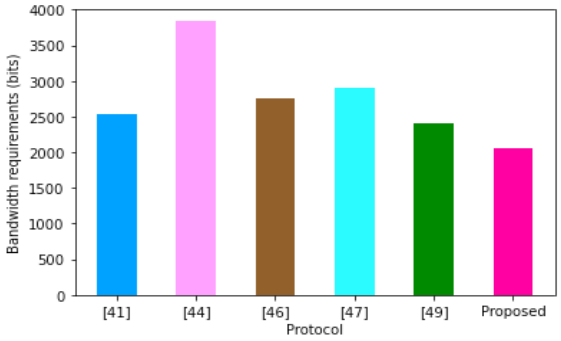

Figure 4. Bandwidth requirements comparisons

Therefore, the proposed algorithm offers strong security protection at the lowest bandwidth requirements.

6. Conclusions and Future Work

Strong security and privacy are critical requirements that must be implemented so as to boost the adoption of WBANs. As such, many protocols have been put forward to protect the mission-critical data exchanged between the body sensors and the remote hospital servers. However, many performance, security and privacy challenges have been noted in majority of the current schemes. Therefore, a truly secure and lightweight authentication algorithm is required to address these gaps. In this paper, a certificate-less authentication algorithm has been presented. Its security analysis has shown that it can offer session key agreement, data privacy, anonymity and untraceability. In addition, its resilience against impersonation, packet replay and man-in-the-middle attacks has been demonstrated. Since this approach has the least execution time and bandwidth requirement, it is the most suitable for deployment in WBANs. Future work will encompass the formal verification of the security features provided by this algorithm.

Conflict of Interest

There is no conflict of interest.

References

[1] Jabeen, T., Ashraf, H., Ullah, A., 2021. A survey on healthcare data security in wireless body area networks. Journal of Ambient Intelligence and Humanized Computing. pp. 1-14.

[2] Ali, S., Ashraf, H., Ramazan, M.S., 2020. An efficient cryptographic technique using modified Diffie-Hellman in wireless sensor networks. International Journal of Distributed Sensor Networks. 16(6), 24.

[3] Farooq, S., Prashar, D., Jyoti, K., 2018. Hybrid encryption algorithm in wireless body area networks (WBAN). Intelligent Communication, Control and Devices. Springer, Singapore. pp. 401-410.

[4] Mehmood, G., Khan, M.Z., Waheed, A., et al., 2020. A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. IEEE Access. 8, 131397-131413.

[5] Nyangaresi, V.O., 2021. ECC based authentication scheme for smart homes. 2021 International Symposium ELMAR, IEEE. pp. 5-10.

[6] Abidi, B., Jilbab, A., Mohamed, E.H., 2020. Journal of Medical Engineering & Technology. 44(3), 97-107.

[7] Hajar, M.S., Al-Kadri, M.O., Kalutarage, H.K., 2021. A survey on wireless body area networks: Architecture, security challenges and research opportunities. Computers & Security. 104, 102211.

[8] Nyangaresi, V.O., Abood, E.W., Abduljabbar, Z.A., et al., 2021. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. 2021 5th International Conference on Information Systems and Computer Networks (ISCON), IEEE. pp. 1-6.

[9] Narwal, B., Mohapatra, A.K., 2021. A survey on security and authentication in wireless body area networks. Journal of Systems Architecture. 113, 101883.

[10] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., et al., 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal. 18(2), 113-122.

[11] Nyangaresi, V.O., Rodrigues, A.J., 2022. Efficient handover protocol for 5G and beyond networks. Computers & Security. 113, 102546.

[12] Fan, S., Li, K., Zhang, Y., et al., 2020. A hybrid chaotic encryption scheme for wireless body area networks. IEEE Access. 8, 183411-183429.

[13] Bashir, A., Mir, A.H., 2018. Securing communication in MQTT enabled Internet of Things with lightweight security protocol. EAI Endorsed Trans. Internet Things. 3(12), 1-6.

[14] Nyangaresi, V.O., Alsamhi, S.H., 2021. Towards secure traffic signaling in smart grids. in 2021 3rd Global Power, Energy and Communication Conference (GPECOM), IEEE. pp. 196-201.

[15] Bhattacharya, P., Tanwar, S., Bodkhe, U., et al., 2019. BinDaaS: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Transactions on Network Science and Engineering. 8(2), 1242-1255.

[16] Cheng, X., Chen, F., Xie, D., et al., 2019. Blockchain-Based Secure Authentication Scheme for Medical Data Sharing. International Conference of Pioneering Computer Scientists, Engineers and Educators, Springer, Singapore. pp. 396-411.

[17] Xu, J., Meng, X., Liang, W., et al., 2020. A Hybrid Mutual Authentication Scheme Based on Blockchain Technology for WBANs. International Conference on Blockchain and Trustworthy Systems, Springer, Singapore. pp. 350-362.

[18] Gupta, R., Tanwar, S., Tyagi, S., et al., 2019. HaBiTs: Blockchain-based Tele-surgery Framework for Healthcare 4.0. 2019 international conference on computer, information and telecommunication systems (CITS), IEEE. pp. 1-5.

[19] Nyangaresi, V.O., Abduljabbar, Z.A., Al Sibahee, M.A., et al., 2021. Towards Security and Privacy Preservation in 5G Networks. 2021 29th Telecommunications Forum (TELFOR), IEEE. pp. 1-4.

[20] Liu, X., Jin, C., Li, F., 2018. An improved two-layer authentication scheme for wireless body area networks. Journal of Medical Systems. 42(8), 1-14.

[21] Sammoud, A., Chalouf, M.A., Hamdi, O., et al., 2020. A new biometrics-based key establishment protocol in wban: energy efficiency and security robustness analysis. Computers & Security. 96, 101838.

[22] Renuka, K., Kumari, S., Li, X., 2019. Design of a secure three-factor authentication scheme for smart healthcare. Journal of Medical Systems. 43(5), 133.

[23] Mwitende, G., Ye, Y., Ali, I., et al., 2020. Certificateless Authenticated Key Agreement for Blockchain-Based WBANs. Journal of Systems Architecture. 110, 101777.

[24] Nyangaresi, V.O., Abduljabbar, Z.A., Refish, S.H.A., et al., 2022. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference, Springer, Cham. pp. 325-340.

[25] Sahoo, S.S., Mohanty, S., Majhi, B., 2020. A secure three factor based authentication scheme for health care systems using IoT enabled devices. Journal of Ambient Intelligence and Humanized Computing. 12(1), 1419-1434.

[26] Pirbhulal, S., Zhang, H., Mukhopadhyay, S.C., et al., 2015. An efficient biometric-based algorithm using heart rate variability for securing body sensor networks. Sensors. 15(7), 15067-15089.

[27] Peter, S., Pratap Reddy, B., Momtaz, F., et al., 2016. Design of secure ECG-based biometric authentication in body area sensor networks. Sensors. 16(4), 570.

[28] Wu, F., Li, X., Sangaiah, A.K., et al., 2018. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 82, 727-737.

[29] Liu, J., Zhang, L., Sun, R., 2016. 1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks. Sensors. 16(5), 728.

[30] Anwar, M., Abdullah, A.H., Butt, R.A., et al., 2018. Securing data communication in wireless body area networks using digital signatures. Technical Journal. 23(02), 50-55.

[31] Nyangaresi, V.O., 2021. Provably Secure Protocol for 5G HetNets. in 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), IEEE. pp. 17-22.

[32] Chang, C.C., Lee, J.S., Wu, J.S., 2017. An Energy Conservation Authentication Scheme in Wireless Body Area Network. Communications of the CCISA. 23(4), 37-54.

[33] Tan, H., Chung, I., 2019. Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. IEEE Access. 7, 151459-151474.

[34] Jegadeesan, S., Azees, M., Babu, N.R., et al., 2020. EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access. 8, 48576-48586.

[35] Shim, K.A., 2018. Comments on "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks". IEEE Transactions on Information Forensics and Security. 15, 81-82.

[36] Xiong, H., Qin, Z., 2015. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE transactions on information forensics and security. 10(7), 1442-1455.

[37] Zhao, Z., 2014. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. Journal of Medical Systems. 38(2), 1-7.

[38] Nyangaresi, V.O., Ibrahim, A., Abduljabbar, Z.A., et al., 2021. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. in 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), IEEE. pp. 1-6.

[39] Zebboudj, S., Cherifi, F., Mohammedi, M., et al., 2017. Secure and efficient ECG-based authentication scheme for medical body area sensor networks. Smart Health. 3, 75-84.

[40] Challa, S., Wazid, M., Das, A.K., et al., 2017. Secure signature-based authenticated key establishment scheme for future iot applications. IEEE Access. 5, 3028-3043.

[41] Ullah, M.G., Chowdhary, B.S., Rajput, A.Q., et al., 2014. Wireless body area sensor network authentication using voronoi diagram of retinal vascular pattern. Wireless Personal Communications. 76(3), 579-589.

[42] Jiang, Q., Lian, X., Yang, C., et al., 2016. A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. Journal of Medical Systems. 40(11), 1-10.

[43] Abina, P., Dhivyakala, K., Suganya, L., et al., 2014. Biometric Authentication System for Body Area Network. Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 3(3), 7954-7964.

[44] Zhou, L., Li, X., Yeh, K.H., et al., 2019. Lightweight iot based authentication scheme in cloud computing circumstance. Future Generation Computer Systems. 91, 244-251.

[45] Nyangaresi, V.O., Ogundoyin, S.O., 2021. Certificate Based Authentication Scheme for Smart Homes. 2021 3rd Global Power, Energy and Communication Conference (GPECOM), IEEE. pp. 202-207.

[46] Farash, M.S., Turkanovi´c, M., Kumari, S., et al., 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Networks. 36, 152-176.

[47] Sharma, G., Kalra, S., 2019. A lightweight user authentication scheme for cloud-IoT based healthcare services. Iranian Journal of Science and Technology, Transactions of Electrical Engineering. 43(1), 619-636.

[48] Wu, L., Zhang, Y., Li, L., et al., 2016. Efficient and anonymous authentication scheme for wireless body area networks. Journal of Medical Systems. 40(6), 1-12.

[49] Wazid, M., Das, A.K., Shetty, S., et al., 2019. LDA-KM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment. Sensors. 19(24), 5539.

[50] Javali, C., Revadigar, G., Libman, L., et al., 2015. SeAK: Secure authentication and key generation protocol based on dual antennas for wireless body area networks. International Workshop on Radio Frequency Identification: Security and Privacy Issues, Springer, Cham. pp. 74-89.

[51] Zhang, W., Qin, T., Mekonen, M., et al., 2018. Wireless body area network identity authentication protocol based on physical unclonable function. 2018 International Conference on Sensor Networks and Signal Processing (SNSP), IEEE. pp. 60-64.

[52] Nyangaresi, V.O., Petrovic, N., 2021. Efficient PUF based authentication protocol for internet of drones. in 2021 International Telecommunications Conference (ITC-Egypt), IEEE. pp. 1-4.

[53] Wang, W., Shi, X., Qin, T., 2019. Encryption-free Authentication and Integrity Protection in Body Area Networks through Physical Unclonable Functions. Smart Health. 12, 66-81.

[54] Xie, L., Wang, W., Shi, X., et al., 2017. Lightweight mutual authentication among sensors in body area networks through Physical Unclonable Functions. 2017 IEEE International Conference on Communications (ICC), IEEE. pp. 1-6.

[55] Tan, X., Zhang, J., Zhang, Y., et al., 2020. A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Science and Technology. 26(1), 36-47.

[56] Alaparthy, V.T., Morgera, S.D., 2018. A multi-level intrusion detection system for wireless sensor networks based on immune theory. IEEE Access. 6, 47364-47373.

[57] Iqbal, J., Umar, A.I., ul Amin, N., et al., 2017. Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks. International Journal of Advanced Computer Science And Applications. 8(7), 180-187.

[58] Li, X., Ibrahim, M.H., Kumari, S., et al., 2017. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks. 129, 429-443.

[59] Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O., 2022. Machine Learning Protocol for Secure 5G Handovers. International Journal of Wireless Information Networks. 29(1), 14-35.

[60] Khan, H., Dowling, B., Martin, K.M., 2018. Highly efficient privacy-preserving key agreement for wireless body area networks. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE. pp. 1064-1069.

[61] He, D., Zeadally, S., 2015. Authentication protocol for an ambient assisted living system. IEEE Communications Magazine. 53(1), 71-77.

[62] Nyangaresi, V.O., 2021. Hardware assisted protocol for attacks prevention in ad hoc networks. in International Conference for Emerging Technologies in Computing, Springer, Cham. pp. 3-20.

[63] He, D., Zeadally, S., Kumar, N., et al., 2016. Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal. 11(4), 2590-2601.

[64] Hady, A.A., Ghubaish, A., Salman, T., et al., 2020. Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access. 8, 106576-106584.

[65] Wang, C., Zhang, Y., 2015. New authentication scheme for wireless body area networks using the bilinear pairing. Journal of Medical Systems. 39(11), 1-8.

[66] Xiong, H., 2014. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Transactions on Information Forensics and Security. 9(12), 2327-2339.

[67] Nyangaresi, V.O., 2021. Lightweight key agreement and authentication protocol for smart homes. 2021 IEEE AFRICON, IEEE. pp. 1-6.

[68] Chia-Hui, L., Yu-Fang, C., 2016. Secure user authentication scheme for wireless healthcare sensor networks. Journal of Computers and Electrical Engineering. 59, 250-261.

[69] Shen, J., Chang, S., Shen, J., et al., 2018. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems. 78, 956-963.

[70] Nyangaresi, V.O., Moundounga, A.R.A., 2021. Secure Data Exchange Scheme for Smart Grids. in 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), IEEE. pp. 312-316.

[71] Srinivas, J., Das, A.K., Wazid, M., et al., 2018. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. IEEE Transactions on Dependable and Secure Computing. 17(6), 1133-1146.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Development of Recovery and Redundancy Model for Real Time Wireless Networks

Boniface Kayode Alese[1] Bamidele Moses Kuboye[2*] Omolara Iyabode Alabede[3]

1. Department of Cybersecurity, Federal University of Technology, Akure, Nigeria
2. Department of Information Technology, Federal University of Technology, Akure, Nigeria
3. Department of Computer Science, Federal University of Technology, Akure, Nigeria

ARTICLE INFO

Article history
Received: 22 July 2022
Revised: 18 August 2022
Accepted: 19 August 2022
Published Online: 31 August 2022

Keywords:
Sequential time division multiple access (S-TDMA)
Wireless
Redundancy
Packets
Media access control (MAC)

ABSTRACT

The growth in wireless technologies applications makes the necessity of providing a reliable communication over wireless networks become obvious. Guaranteeing real time communication in wireless medium poses a significant challenge due to its poor delivery reliability. In this study, a recovery and redundancy model based on sequential time division multiple access (S-TDMA) for wireless communication is developed. The media access control (MAC) layer of the S-TDMA determines which station should transmit at a given time slot based on channel state of the station. Simulations of the system models were carried out using MATLAB SIMULINK software. SIMULINK blocks from the signal processing and communication block sets were used to model the communication system. The S-TDMA performance is evaluated with total link reliability, system throughput, average probability of correct delivery before deadline and system latency. The evaluation results displayed in graphs when compared with instant retry and drop of frame were found to be reliable in recovering loss packets.

1. Introduction

Ascertaining an unhindered real-time delivery in wireless communication medium is challenging. It has poor delivery reliability compared to wired networks [1]. Real-time applications in wireless broadcast have stringent and short transfer deadline thereby making packet loss recovery more difficult [2]. Real-time communication is the application that demands a certain quality of service (QoS) to the communication network like maximum delay, maximum loss rate upon its connection to guarantee the requested service quality [3]. The real-time measurement of a network is its ability to carry information for given time limit. In other words, real-time information has to be received by the recipient before a certain deadline [4]. Some important features of real time applications as discussed

*Corresponding Author:
Bamidele Moses Kuboye,
Department of Information Technology, Federal University of Technology, Akure, Nigeria;
Email: bmkuboye@futa.edu.ng

DOI: https://doi.org/10.30564/jcsr.v4i3.4915

in Al-Kuwaiti [5] are timeliness, peak load design, predictability, fault tolerance and maintainability.

Time division multiple access (TDMA) approach has been proving useful in resolving the issue of medium contention and frame collisions but frame reception remains unpredictable as a result of its dynamic and shared nature of the medium [1]. Real-time MAC protocol uses TDMA to provide stations with a mechanism to reserve a transmission slot in a TDMA cycle of network. The calculation of the required transmission time needs to take into account the number of retransmissions that may be required to achieve a given reliability. The wireless shared nature allows transmissions to be intercepted by noise in the environment. Such interference is commonly addressed by using protocols like TDMA.

In wireless networks, media access control (MAC) protocols like carrier-senses multiple access with collision avoidance (CSMA/CA), multiple access with collision avoidance (MACA) are liable to contention and collisions because of different attempting stations to access the medium the same time [6]. Hence, TDMA channel access approach provides collision and contention-free medium access. Transmission errors occur simply due to background noise, transient propagation effects and so on. Burst errors characterized by a distribution of occurrence and distribution of length of a burst are detected as frame losses [1,7]. Wireless Frame losses are unavoidable; therefore, its recovery effectiveness is important. As soon as burst errors condition lead to the loss of frame(s), the station transmitting must retransmit the affected frame(s) in a way to minimize its possible re-occurrence and still reduce its impact on frames to other destinations. The instant retry approaches, probabilistic backoff, fixed-delay backoff, exponential backoff, frames re-queuing, link quality estimate, congestion awareness, packet rejection estimation and drop of frame approaches have all been used [8,9].

In designing a proficient MAC protocol for wireless networks, the characteristics like energy efficiency, scalability, adaptively, latency, channel utilization, throughput and fairness must be considered [10,11]. Collision occurs in wireless networks once two nodes transfer data at a time over transmission medium. Such problem can be addressed by employing MAC protocol to mediate access to the shared medium to avoid data collision and maintain a fairly efficient sharing of the bandwidth resources. The retransmissions approach may be alright for shared wired media but not over wireless media. The signals to two destinations over a wireless medium will broadcast over diverse paths and meet with different environmental factors. This may results to failed transmission to station A but successful for station B at the same time. Due to these observations, a retransmission protocol that takes into account the characteristics of wireless medium and attempts to re-order the transmission queue following failed transmissions is proposed. This work was designed and implemented using Simulink simulator in Matlab.

The rest of this paper is organized thus: Section 2 and 3 reviews the related literature and describes the design of the S-TDMA system model respectively. Section 4 describes the analysis of performance metric used while section 5 addresses simulation of the system model. The conclusion drawn from the study forms the final section.

2. Related Works

Fault recovery and redundancy in real-time wireless TDMA was studied by Gleeson and Weber [1]. The paper addresses the problem of message delivery reliability in real-time, wireless communication systems, as well as, probabilistic admissions control protocol provision. Two hybrid approaches were used to make the satisfaction of real-time guarantees in on-time packet delivery. These are admissions control and an exponential backoff. Admission control ensures that transmission time is reserved so as to make retransmissions possible while an exponential backoff process rescheduled failed transmissions on a station-by-station basis. The work ensures that the real-time was guaranteed while allowing a limited loss of frames. Ali et al. [11] proposed distortion-based slice level prioritization for real-time video over QoS-enabled wireless networks. The work showed that given a higher-priority to some classified packets in accessing the wireless media, a considerable quality was achieved when prioritization is not used.

A self-regulated redundancy control scheme for high-bit-rate video transmission using packet-level forward-error-correction (FEC) codes over error-prone wireless networks was presented by Shih et al. [12]. Packet-level FEC was used for the self-regulated redundancy scheme to support the high-speed video transmission in wireless networks. The proposed scheme protects video streams from wireless losses as well as controls the redundancy degree to reduce the adverse effect of FEC efficiency. Bassey et al. [13] examined mitigating effect of packet losses on real-time video streaming using peak signal-to-noise ratio (PSNR) as video quality assessment metric. Real-time live video content streaming over the Internet is complicated as a result of bandwidth, jitter, packet losses and fair sharing of network resources among users. The work uses PSNR as video quality assessment metric to moderate packet losses on real-time video streaming. The video frame rates were compressed and the results showed the higher the PSNR, the lower the loss rate, and the bet-

ter the video quality.

Wang et al. [14] studied hybrid recovery strategy based on random terrain (HRSRT) in wireless sensor networks. It was stated that getting fruitful data collection and aggregation is main goal for a broad spectrum of wireless sensor networks applications but connectivity loss in a network may bring failure in data aggregation. The work uses HRSRT that takes both realistic terrain influences and quantitative limitations of relay devices into consideration. The simulation results showed that HRSRT performs better in terms of overall energy cost. Modular redundancy for cloud based IP multimedia subsystem (IMS) robustness was explored by Raza et al. [15]. IMS is an emerging communication framework that provides a wide range of multimedia services such as video over LTE, interactive gaming in active LTE network. Due to the emerging applications support, network operators are embracing cloud-based IMS and are deploying it to meet the need of increasing multimedia traffic demand. This paper revealed that cloud-based IMS cannot provide session-level resilience under faults. The origin of the problem stems from the weak failure recovery mechanisms. In other to solve this, fault-tolerance design to IMS control-plane processes was proposed. The outcomes showed that session-level resilience can be achieved by carrying out fail-over procedure within tens of milliseconds under different combinations of IMS control-plane operations failures.

Hybrid cross layer fault resilient energy efficient data transmission for underwater acoustic sensor networks was done by Vidyalakshmi et al. [16]. The solution proposed in this work ensures high packet delivery ratio with low energy consumption. According to the experimental analysis, the proposed work out-performs the existing works when considering packet delivery ratio, life time as well as network overhead. Arefi and Khabbazian [2] examined packet loss recovery in broadcast for real-Time applications in dense wireless networks. This work introduces random instantly decodable network coding (RIDNC) which is a random encoding approach to instantly decodable network coding (IDNC) which was referred to as random IDNC encoder (RACE). It was observed that RACE compared with the CrowdWiFi encoder using simulations, recovers more lost packets.

He and Zhou [17] presented real-time data recovery in wireless sensor networks (WSN) using spatiotemporal correlation based on sparse representation. Historical data, joint low-rank constraint and temporal stability were used as data for spatiotemporal correlation. The simulation results showed the proposed method beats the compressed sensing (CS) method with sparse sensing matrix, joint CS and matrix completion method. Lucas-Estañ et al. [18] studied a work on redundancy and diversity in wireless networks. The work supported mobile industrial applications in Industry 4.0 otherwise known as Factories of the Future (FoF). Evaluation through simulation reveals how the capacity of diversity and redundancy improve the reliability and latency of wireless networks for mobile industrial applications. Kim et al. [19] presented a survey on real-time communications in wireless sensor networks. It presented the up-to-date research approaches and discussed some features that are important to real-time communications networks in wireless sensor. It was partitioned into hard, soft, and firm real-time model. It was observed that MAC scheduling and routing were common to all the categories. The work concluded with suggestions to potential directions for future research.

3. Design of the S-TDMA System Model

In this study, a recovery and redundancy model for wireless communication using sequential TDMA (S-TDMA) is designed. The S-TDMA MAC-layer determines which station should be allowed to transmit at an allotted time slot based on the channel state of the station. The S-TDMA time slot scheme for 6 stations is shown in Figure 1. Each station is given a time slot to transmit. A slot is a super frame which contains the beacon frame (BC), data frames of varying sizes and reserved frames for retransmission in case of failed detection. The beacon is used to distinctively identify the super frame and its transmitter. Each time slot in the S-TDMA cycle is of fixed size and a station can use any of the available slots to transmit. The flowchart for the designed S-TDMA model is presented in Figure 2.

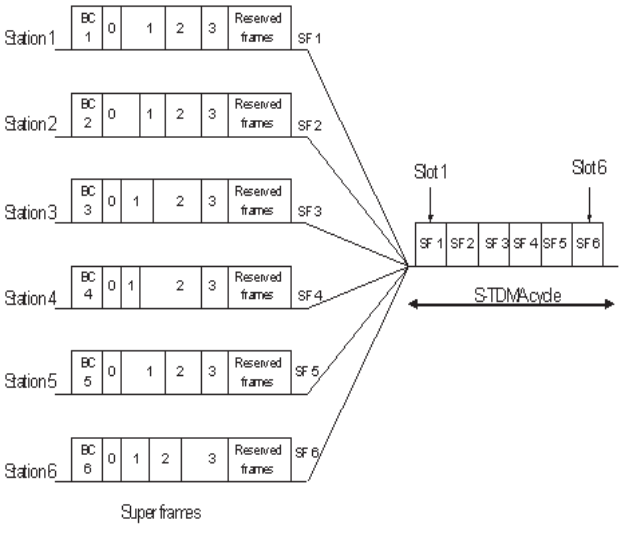

Figure 1. S-TDMA Time Slot Scheme in MAC Layer

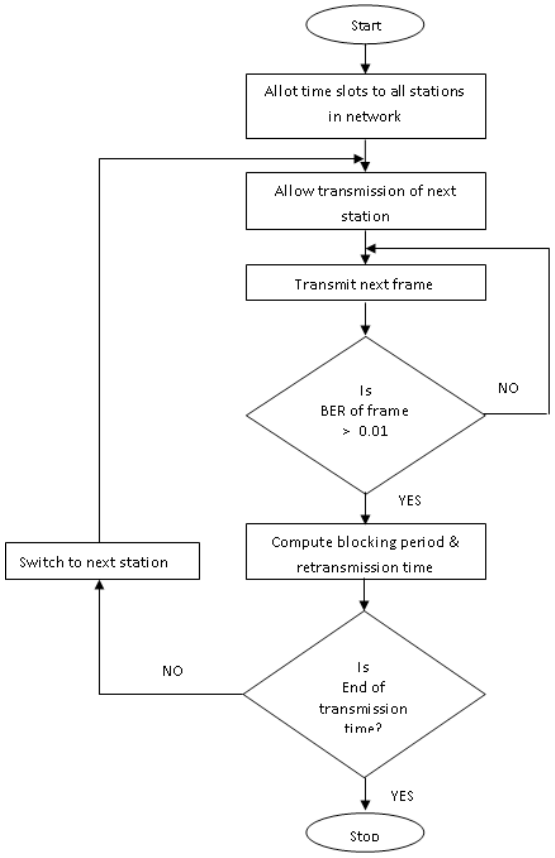

Figure 2. Flowchart of the designed S-TDMA

4. Performance Metric analysis

The performance of the designed S-TDMA model was based on these performance metrics: total link reliability (TLR), throughput (τ), average probability of correct delivery before deadline ($\overline{P}_d$) and system latency (L). These metrics are described in this section and they are used to measure the degree of quality-of-service (QoS) of the system.

Total Link Reliability (TLR)

Link reliability is a measure of the success of data transmissions in a wireless communication system. A reliable wireless communication link ensures the information data transmitted from the source is received correctly at the sink without any data loss.

Assuming a station n transmitted some frames, then, the total sum of frames successfully transferred is given in Equation (1):

$$F_{succ}(n) = \sum_i n_i \tag{1}$$

where $F_{succ}(n)$ is the total number of frames successfully transmitted by station, thus, the probability that some frames are lost during transmission is obtained in Equation (2):

$$p_{loss}(n) = \frac{\{F_{rq} - F_{succ}(n)\}}{F_{rq}} \tag{2}$$

where $p_{loss}(n)$ is the frame loss probability and F_{rq} stands for the required number of frames to be transmitted successfully.

The TLR of the wireless network is the sum of the link reliabilities of all the stations utilizing the network and hence, the total link reliability for the network is expressed using Equation (3):

$$TLR = \frac{1}{N}\sum_{n=1}^{N} LR(n) \times 100\% \tag{3}$$

where N is the total stations, therefore, link reliability for the n^{th} station is obtained in Equation (4) [20]:

$$LR(n) = 1 - p_{loss}(n) \tag{4}$$

where $p_{loss}(n)$ had been defined earlier in Equation (2).

System throughput (τ)

System throughput is defined as the rate of transmission of data packets by the system. It depends on the number of data successfully transmitted within a given period of time, and it is measured in megabits per second (Mbps). The system throughput is expressed in Equation (5):

$$\tau = \frac{\text{total packets successfully tramsmitted}}{\text{Maximun transmission time}} \tag{5}$$

Average probability of correct delivery before deadline ($\overline{p}_d$)

A recovery MAC protocol would request retransmission of the frames that are not correctly received by the transmitting station,, thus, a specific time is assigned for this transmission, however, the station may not be able to retransmit successfully till this time elapses.

The probability of correct delivery of frames before deadline by station n can be expressed using Equation (6):

$$p_d(n) = \frac{1}{R}\sum_i \left[1 - p_f(i)\right] \tag{6}$$

where the probability of a frame of station n failing on the i^{th} attempt is given in Equation (7):

$$p_f(i) = P_e(i)^{(R-1)+1} \tag{7}$$

But $p_e(i)$ is error probability or BER and R is number of retransmissions.

Therefore, when considering all the stations in the network, the average probability of correct delivery before deadline will be expressed Equation (8).

$$\overline{p}_d = \frac{1}{N}\sum_{n=1}^{N} p_d(n) \tag{8}$$

where N is the summation of stations in the network [20].

Meanwhile, error probability (p_e) or BER is calculated in the simulation using Equation (9):

$$BER = \frac{\text{number of error or corrupted bits}}{\text{total number of hits transmitted}} \quad (9)$$

System Latency (L)

System latency is the time delay experienced by the system in successfully transmitting a given volume of data, therefore any system that gives moderately low or negligible latency is assumed to be fast. It is commonly expressed in milliseconds and can be given using Equation (10):

$$L = \frac{\text{total time taken}}{\text{total packets successfully transmitted}} \quad (10)$$

5. Simulation of the System Model

The models simulations were carried out using MATLAB/SIMULINK. SIMULINK blocks from the signal processing and communication blocksets were used to model the communication system. Table 1 shows the parameter used for the models simulation. MATLAB was utilized in this study because of its ease of use and graphical presentation of results.

Table 1. Simulation Parameters for the three Models

Parameters	Model		
	Instant retry	Drop of frame	S-TDMA
Maximum Number of Stations	6	6	6
Maximum Number of Packets	100	100	100
Maximum number of retransmission	NA	3	NA
Frame length	50	50	50
Blocking period	0 ms	0 ms	200 ms
Time slot per station	180 ms	180 ms	180 ms
Modulation type	MPSK	MPSK	MPSK
Modulation order	4	4	4

System Total Link Reliability

The developed S-TDMA model is compared with two of the existing models namely drop-of-frame and instant retry. Figure 3 shows the performances of three models in relations to total link reliability. Link reliability is a measure of the success of data transmissions in a wireless communication system. The total link reliability results of the drop-of-frame model for stations of 2, 3, 4, 5 and 6 networks are 93.00%, 92.67%, 91.50%, 94.40%, 94.00% respectively. The results reveal that the total link reliability of the drop-of-frame model is dependent on how many of the stations are effective in the network and not necessarily the number of stations utilizing the channel.

For the instant retry model, the total link reliability for stations of 2, 3, 4, 5 and 6 are 84.00%, 85.33%, 97.00%, 92.80% and 96.00% respectively. These results for the instant retry model also reveal that though the reliability tends to increase with increasing number of stations, the total link reliability is dependent on how many of the stations are effective in the network and not necessarily the number of stations utilizing the channel. For the S-TDMA model, the total link reliability for stations of 2, 3, 4, 5 and 6 are 100%, 100%, 100%, 100% and 100%, respectively. This reveals that in the S-TDMA model, all the transferrable data were successfully transmitted during the transmission period unlike the other two models where some of the frames could not be transmitted before the transmission period elapsed. The developed S-TDMA model is able to achieve this because each Station consists of a backup transmitter in case the main transmitter fails to start transmission immediately the channel is open for the station by the MAC controller. This process helps to handle redundancy at each station in the communication network, thereby, eliminating downtime.

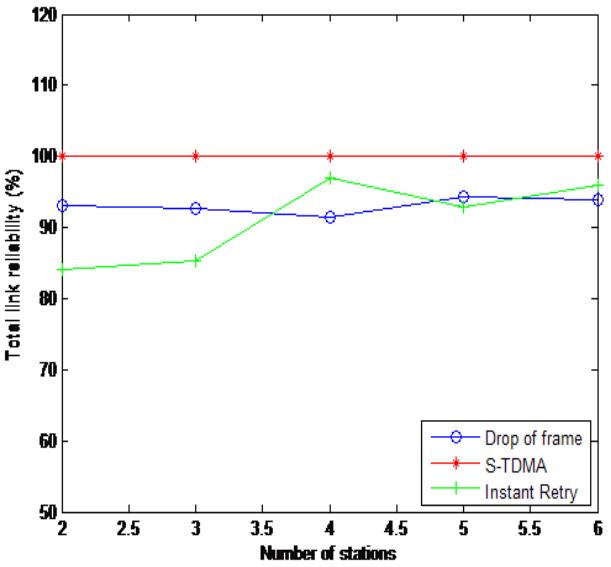

Figure 3. Total link reliability

System Throughput

System throughput is the rate of transmission of data packets by the system. The system throughput performances for the models are compared in Figure 4. The system throughputs in the drop-of-frame model for stations of 2, 3, 4, 5 and 6 are 3.1667 Mbps, 3.1556 Mbps, 3.1167 Mbps, 3.8800 Mbps and 3.7667 Mbps respectively. This shows that the system throughput in the drop-of-frame model is independent of the number of stations in the network. The system throughputs in the instant retry model for stations of 2, 3, 4, 5 and 6 are 2.8000 Mbps, 2.8444 Mbps, 3.2333 Mbps, 3.0933 Mbps and 3.2000 Mbps respectively. This also shows that the system throughput in

the instant retry model is independent of the number of stations in the network. However, the drop-of-frame model gives relatively higher throughput than the instant retry model. This is because the drop-of-frame model drops any frame that would cause redundancy for the system to keep transmitting without delay but with a tradeoff of lost frames. The system throughputs in the S-TDMA model for stations of 2, 3, 4, 5 and 6 are 3.3333 Mbps, 3.3333 Mbps, 3.3333 Mbps, 3.3333 Mbps and 3.3333 Mbps respectively. These results also reveal that the system throughput in the S-TDMA model is not dependent stations number in the network. However, the S-TDMA gives relatively higher throughput than both the drop-of-frame and instant retry models. This is because the S-TDMA model allocates transmission and a retransmission period dynamically depending on the state of the networks, which helps to eliminate redundancy in the network and also ensures that all the frames are successfully transmitted.

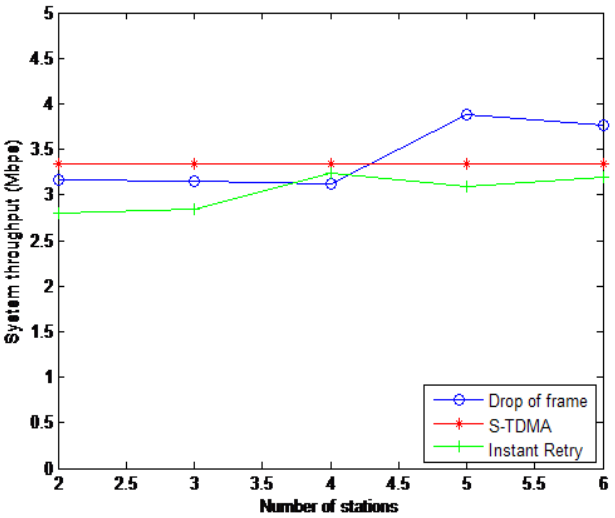

Figure 4. System throughput

Probability of Correct Delivery

This is the average probability of correct delivery of frames before deadline by any station. Figure 5 presents the performances of the models in terms of average probability of correct delivery before deadline. For stations of 2, 3, 4, 5 and 6, the drop-of-frame model gives 0.9500, 0.9467, 0.9350, 0.9640 and 0.9600 respectively. The instant retry model gives 0.9919, 0.9926, 0.9910, 0.9950 and 0.9955 for stations of 2, 3, 4, 5 and 6 respectively. The S-TDMA model gives 0.9949, 0.9936, 0.9905, 0.9894 and 0.9949 for stations of 2, 3, 4, 5 and 6 respectively. From the results, the Instant retry model gives relatively higher average probability of correct delivery when compared to the drop-of-frame model. This is because the drop-of-frame model drops redundant frames thereby losing then during transmission, while the instant retry model keeps trying to retransmit the redundant frames until they finally get to the receiving end; and this gives more success to the instant retry model in terms of frame delivery. However, the S-TDMA model gives relatively similar average probability of correct delivery performance when compared to the instant retry model. This is because the S-TDMA model also ensures that every frame gets to the receiving end.

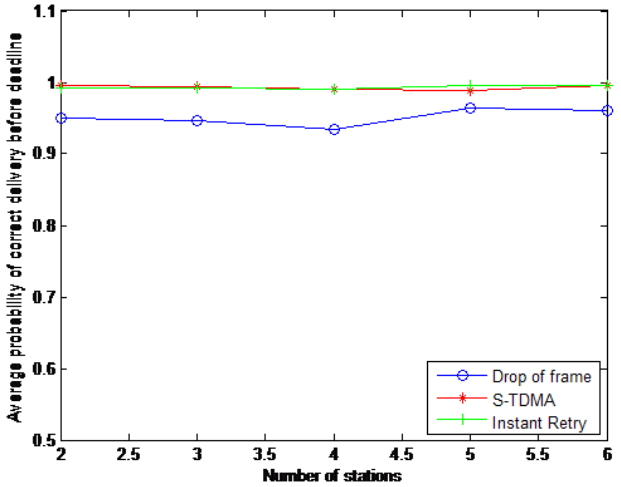

Figure 5. Average probability of correct delivery before deadline

System Latency

The performances of the models in terms of system latency were presented in Figure 6. System latency is the time delay experienced by the system in successfully transmitting a given volume of data. This is measured in milliseconds. For stations 2, 3, 4, 5 and 6, the drop-of-frame model gives 0.3158, 0.3169, 0.3209, 0.2577 and 0.2655, respectively. The instant retry model gives 0.3571, 0.3516, 0.3093, 0.3233 and 0.3125 for the stations of 2, 3, 4, 5 and 6 respectively. The S-TDMA model gives 0.3000, 0.3000, 0.3000, 0.3000 and 0.3000 for the stations of 2, 3, 4, 5 and 6 respectively. These results reveal that the system latency for the drop-of-frame model is relatively lower than that of the instant retry model. This is due to the fact that the instant retry model experiences more delay in trying to repeatedly retransmit a redundant frame, while the drop-of-frame eliminates the delay by dropping any redundant frame so as to allow the active ones to utilize the channel at any time period. The system latency for the S-TDMA is however shown to be constant for all the number of stations considered in the network and the latency is relatively higher than those of drop-of-frame for 5 stations and 6 stations. This implies that for the S-TDMA model, the system latency is independent of the number

of stations in the network; however, the drop-of-frame reduces system latency with increasing number of stations when compared to both the S-TDMA and instant retry models.

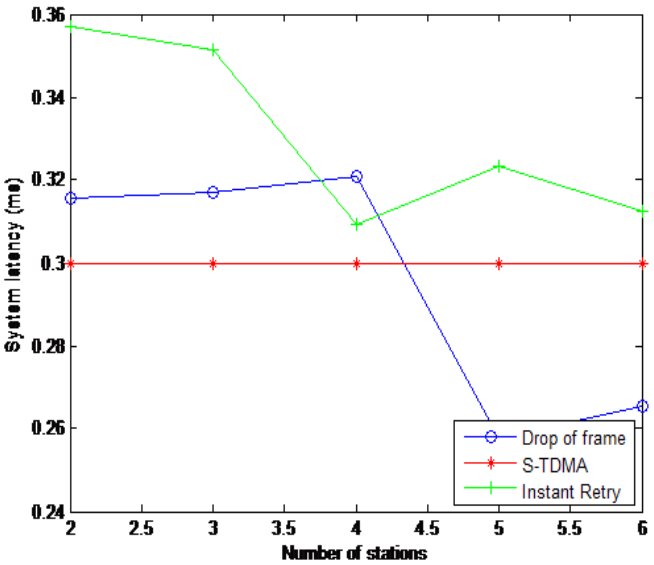

Figure 6. System latency

6. Conclusions

In this study, S-TDMA designed model is used as a recovery and redundancy model for real time wireless network. The model utilizes MAC protocol based on TDMA and the MAC layer of the S-TDMA to determine which station should be permitted to transmit at a given time slot based on the channel state of the station. The S-TDMA system model was simulated with MATLAB SIMULINK. The model is compared with two other existing models; drop of frame and instant retry. The metrics used to evaluate the performance of the designed S-TDMA are total link reliability, system throughput, average probability of correct delivery before deadline and system latency. The results of the metrics are displayed in graphs and tables. These metrics give the degree of Quality of Service (QoS) delivery of the system. The developed program is tested and found to be reliable in recovery of loss packets. Since the designed model has been able to provide an effective means of recovering loss frames, it is therefore recommended to be used by industries in order to combat the problem of message delivery reliability in wireless network since it performs better than other existing models.

Conflict of Interest

There is no conflict of interest.

References

[1] Gleeson, M., Weber, S., 2008. Fault Recovery and Redundancy in Real-time Wireless TDMA. (Accessed on February 22, 2022).

[2] Arefi, A., Khabbazian, M., 2019. Packet Loss Recovery in Broadcast for Real-Time Applications in Dense Wireless Networks from arXiv:1911.08449v1 (Accessed on19 Nov 2019).

[3] Stankovic, J., Ramamritham, K., 1988. Hard real-time systems. Tutorial text, IEEE Computer press.

[4] Deepali, V., Satbir, J., 2011. Real Time Communication Capacity for Data Delivery in Wireless Sensor Networks.

[5] Al-Kuwaiti, M., Kyriakopoulos, N., Hussein, S., 2009. Comparative Analysis of Network Dependability,Fault-tolerance, Reliability, Security, and Survivability. IEEE Communications Surveys & Tutorials. 11(2).

[6] Samant, T., Kumar, Y.S., Swayamsiddha, S., 2020. Comparison Analysis of MAC Protocols for Wireless Sensor Networks. IGI Global.

[7] Pijus, K., Punyasha, C., 2014. A Survey on TDMA-based MAC Protocols for Wireless Sensor Network. International Journal of Emerging Technology and Advanced Engineering. 4(6). www.ijetae.com.

[8] Chatterjee, P., Das, N., 2009. A Cross-Layer Distributed TDMA Scheduling for Data Gathering with Minimum Latency in Wireless Sensor Networks: IEEE Wireless, VITAE.

[9] Lee, H.J., Cerpa, A., Levis, P., 2007. Improving wireless simulation through noise modeling. IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks. pp. 21-30.

[10] Ye, W., Heidemann, J., Estrin, D., 2002. An energy-efficient MAC protocol for wireless sensor networks. IEEE Infocom. pp. 1567-1576.

[11] Ali, I.A., Fleury, M., Ghanbari, M., 2012. Distortion-Based Slice Level Prioritization for Real-Time Video over QoS-EnabledWireless Networks. Advances in Multimedia. Article ID 319785. pp. 9. DOI: https://doi.org/10.1155/2012/319785

[12] Shih, C.H., Tou, Y.M., Shieh, C.K., et al., 2015. A Self-Regulated Redundancy Control Scheme for Wireless Video Transmission. IEEE.

[13] Bassey, A., Udofia, K.M., Uko, M.C., 2016. Mitigating the Effect of Packet Losses on Real-Time Video Streaming using Peak Signal-To-Noise Ratio (PSNR) as Video Quality Assessment Metric. European Journal of Engineering and Technology. 4(3).

[14] Wang, X., Xu, L., Zhou, S., et al., 2017. Hybrid Recovery Strategy Based on Random Terrain in Wireless Sensor Networks. Scientific Programming, Article ID 5807289, pp. 19.
DOI: https://doi.org/10.1155/2017/5807289

[15] Raza, M.T., Tseng, H., Li, C., et al., 2017. Modular Redundancy for Cloud based IMS Robustness. MobiWac'17, Miami, FL, USA.

[16] Vidyalakshmi, K., Siddappa, M., Shanmukha, B., 2019. Hybrid Cross Layer Fault Resilient Energy Efficient Data Transmission for Underwater Acoustic Sensor Networks. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 8(12).

[17] He, J., Zhou, Y., 2019. Real-Time Data Recovery in Wireless Sensor Networks Using Spatiotemporal Correlation Based on Sparse Representation. Wireless Communications and Mobile Computing. Article ID 2310730, pp. 7.

[18] Lucas-Estañ, M.C., Coll-Perales, B., Gozalvez, J., 2020. Redundancy and Diversity in Wireless Networks to Support Mobile Industrial Applications in Industry 4.0. IEEE Transactions on Industrial Informatics. 17(1), 2021.
DOI: http://dx.doi.org/10.1109/TII.2020.2979759

[19] Kim, B., Park, H., Kim, K.H., et al., 2017. A Survey on Real-Time Communications in Wireless Sensor Networks. Wireless Communications and Mobile Computing. Article ID 1864847, pp. 14.
DOI: https://doi.org/10.1155/2017/1864847

[20] Ma, M., Yang, Y., 2007. SenCar: An Energy-Efficient Data Gathering Mechanism for Large-Scale Multihop Sensor Networks, IEEE Transactions on Parallel and Distributed Systems.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

REVIEW

The Internet of Things Security and Privacy: Current Schemes, Challenges and Future Prospects

Peter Sungu Nyakomitta* **Solomon Ogara** **Paul Abounji**

Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya

ARTICLE INFO

Article history
Received: 26 July 2022
Revised: 2 September 2022
Accepted: 5 September 2022
Published Online: 13 September 2022

Keywords:
IoT
Security
Privacy
Attacks
Performance

ABSTRACT

The Internet of Things devices and users exchange massive amount of data. Some of these exchanged messages are highly sensitive as they involve organizational, military or patient personally identifiable information. Therefore, many schemes and protocols have been put forward to protect the transmitted messages. The techniques deployed in these schemes may include blockchain, public key infrastructure, elliptic curve cryptography, physically unclonable function and radio frequency identification. In this paper, a review is provided of these schemes including their strengths and weaknesses. Based on the obtained results, it is clear that majority of these protocols have numerous security, performance and privacy issues.

1. Introduction

The Internet of Things (IoT) facilitates data sharing among numerous devices and people through a variety of wireless sensors and mobile computing devices [1-3], as shown in Figure 1. As shown here, the IoT building blocks include the smart things, gateways, middleware and applications. Over the recent past, IoT has acted as an enabling technology in a number of application domains such as healthcare, smart homes, military, weather forecasting, smart cities, fire monitoring and intelligent transport systems. As explained by Mamdouh et al. [4], IoT plays a crucial role in the healthcare where it has helped enhance the quality of life. For instance, Internet of Health Things (IoHT) sensors can perceive biomedical data such as blood pressures and heart [5].

An intruder can attack these sensors and cause the death of a patient. In an IoT environment, privacy and security are major issues that need to be upheld during the communication process. As pointed out by Hassan [6],

*Corresponding Author:
Peter Sungu Nyakomitta,
Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya;
Email: pnyakomitta@yahoo.com

DOI: https://doi.org/10.30564/jcsr.v4i3.4925

numerous security gaps lurk that can permit malicious devices and users to gain access to the IoT resources. In addition, this breach can lead to privacy violations as well as economic losses [7]. This can further enable the adversary to use the hijacked devices as vectors to invade the entire network [8]. These security challenges are attributed to vulnerabilities in the authentication procedures [9,10]. According to Wang et al. [11], the susceptibilities in IoHT can threaten the lives of the patients. For instance, eavesdropping, Sybil, man-in-the-middle (MitM), Distributed Denial of Service (DDoS) and spoofing are serious threats in IoT [12]. There is therefore need to uphold high security in terms of availability, confidentiality and integrity for the sensitive data that is being exchanged. Unfortunately, most of the IoT devices are resource constrained in terms of memory, energy, storage, computation, processing capacity and communication capabilities [13,14]. As such, only lightweight security solutions are feasible in an IoT environment [15]. In this paper, an extensive review of the state of the art schemes that have been developed to address security and privacy issues in IoT are investigated.

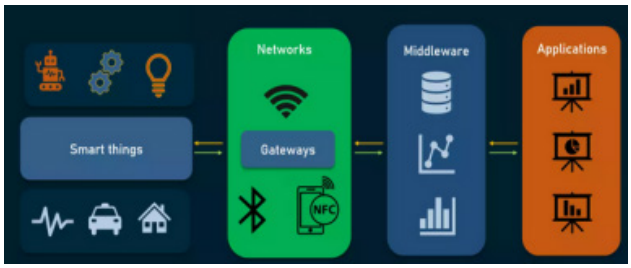

Figure 1. IoT communication architecture

2. Related Work

There have been numerous security solutions developed for an IoT environment, based on techniques such as Physically Unclonable Function (PUF), blockchain, Public Key Infrastructure (PKI), radio frequency identification (RFID) tags among others. For instance lightweight PUF-based identity verification schemes have been presented by Zhao et al. [16], Braeken [17], and Xu et al. [18]. Some of these schemes have been shown to be resilient against replay, cloning and de-synchronization attacks [18]. However, PUF-based schemes have stability issues [19]. On the other hand, blockchain based protocols has been deployed to enhance privacy and identity management in IoT [20-23]. These schemes protect IoT devices against attacks such as cache misappropriation and data modifications [21]. In addition, they offer transparency, time immutability, decentralization and high security for shared data. However, blockchain technology has high computation and storage overheads [24]. Although the RFID-based schemes can secure the IoT communication, they are vulnerable to jamming and cloning attacks [25,26].

On the other hand, PKI-based scheme is presented by Jia et al. [27], while an elliptic curve cryptography (ECC) is introduced by Cheng et al. [28]. However, PKI is a centralized authentication approach hence presents a single point of failure. In addition, it has high communication and computation complexities [29], and cannot resist DoS attacks [30,31]. Although the scheme by Cheng et al. [28] is robust against MitM, replay and impersonation attacks, it has high communication costs. A multiparty access authentication mechanism for IoT has been developed by Zhang et al. [32]. However, this protocol is susceptible to modification, replay, MitM and impersonation attacks. The multi-party access mechanism by Zhang et al. [32] also incurs high processing overheads [33] when large numbers of IoT devices are deployed. This problem can be addressed by the protocol developed by Ali et al. [34], which is shown to have less computation overheads and high throughputs. On the other hand, an identity based scheme is presented by Jiang et al. [35] which does not call for certificates storage.

Although the scheme developed by Jesus et al. [36] boosts security and privacy in IoT, it has elongated latencies. Similarly, the technique by Dittmann and Jelitto [37] enhances end-to-end trust between IoT devices but was never evaluated against DDoS [38]. This attack is prevented by the scheme presented by Das et al. [39]. Although the protocol in Al-Jaroodi et al. [40] can offer secure collection and storage of sensitive data, it does not incorporate any form of authentication between the IoHT users and devices. On the other hand, cross-heterogeneous domain authentication protocol is developed by Yuan et al. [41] incurs high computation and communication overheads.

By deploying the key update strategy, a mutual authentication scheme is developed by Naija et al. [42]. However, this approach cannot withstand jamming attacks [43]. To offer better performance and meet security requirements, a radio frequency fingerprint device authentication approach is presented by Tian et al. [44]. However, security and attack analysis of this scheme is lacking. A Certificate Authority (CA) based authentication technique is presented by Yao et al. [45]. However, certificate maintenance in this protocol is complex.

On the other hand, the identity management scheme in Omar and Basir [46] does not present performance evaluation. Similarly, the machine learning based automated identity confirmation algorithm by Poulter et al. [47] has scalability limitations. Although this federated learning based achieves high privacy during the authentication process, it has high energy consumptions [48].

A novel ECC-based pairing free certificateless signature scheme is developed by Shen et al. [49]. Unfortunately, this technique is susceptible to jamming and DoS attacks. To offer enhanced key exchange between IoT devices, an authentication protocol is presented by Alzahrani et al. [50], which is devoid of third-party involvement [51]. On the other hand, an IoHT device authentication approach is developed by Rathee [52] while an IoT node roaming-based authentication model is presented by Wan et al. [53]. Although this protocol prevents replay and malicious nodes attacks, it has high authentication delays when the number of IoT devices increase.

3. Results

The review of the current security solutions has revealed a number of challenges associated with the current schemes. Table 1 presents the summary of these challenges. Based on the information in Table 1, it is clear that the assurance of perfect security and privacy at optimum performance is still challenging.

Table 1. Summary of challenges of current schemes

Scheme	Challenges
Zhao et al. [16] Braeken [17] Xu et al. [18]	PUF-based schemes have stability issues
Ding et al. [20] Yang et al. [21] Singh [22] Jabbar et al. [23]	Blockchain technology has high computation and storage overheads
Jia et al. [27]	Presents a single point of failure; it has high communication and computation complexities; cannot resist DoS attacks
Cheng et al. [28]	Has high communication costs
Zhang et al. [32]	Is susceptible to modification, replay, MitM and impersonation attacks; incurs high processing overheads
Jesus et al. [36]	Has long latencies
Dittmann and Jelitto [37]	Is never evaluated against DDoS
Al-Jaroodi et al. [40]	Does not incorporate any form of authentication between the IoHT users and devices
Yuan et al. [41]	Incurs high computation and communication overheads
Naija et al. [42]	Cannot withstand jamming attacks
Tian et al. [44]	Lacks security and attack analysis
Yao et al. [45]	Certificate maintenance in this protocol is complex
Omar and Basir [46]	Does not present performance evaluation
Poulter et al. [47]	Has scalability limitations
Shen et al. [49]	Is susceptible to jamming and DoS attacks
Wan et al. [53]	It has high authentication delays when the number of IoT devices increase

Some of the identified issues revolve around certificate management, output stability, single point of failure, DoS, DDoS, modification, jamming, replay, MitM, lack of authentication, long latencies, impersonation, and high complexities in terms of computation, storage overheads and communication overheads. It is also evident that some of these schemes also lack security and attack analysis. Table 2 presents the layered approach of these security, performance and privacy setbacks. It is evident from Table 2 that each and every entity in the IoT infrastructure has some issues that need to be solved.

Table 2. Layered IoT Challenges

Category	Challenges
IoT devices	Authorization, authentication, performance
Application	Authentication, trust, performance, authorization
Data	Trust, privacy
Network	Eavesropping, interception, availability

To address some of these performance, security and privacy shortcomings, the recommendations in the sub-section that follows are deemed necessary.

4. Recommendations

In light of the above IoT security, performance and privacy challenges, the following technologies and procedures are recommended as possible solutions.

Machine learning: In an IoT environment, machine learning (ML) algorithms can be deployed for the detection and prediction of attacks. This can be achieved by monitoring the encryption key size as well as the utilized protocols. This can potentially prevent zero-day attacks, misuse as well as abnormal patients' behavior using their profiles. These profiles can then be stored as signatures in databases to be deployed by security solutions such as next generation firewalls. When utilized at the perception layer, these ML algorithms can perform device authentication to thwart the transmission of false information such as malicious identities.

Separation of access privileges: In this approach, the IoT administrators have distinct privileges to the devices and sensors. This is achieved by having passwords that are quite different from those of the IoT devices. Since recalling all these passwords is challenging, Single Sign On (SSO) technique is used to identify these administrators. This allows for the migration of these passwords with device passwords, facilitating different permissions and policies to offer diverse levels of privileges to access IoT devices. It therefore becomes possible to utilize one unique identity to access multiple services from these IoT devices.

Digital signature: In an IoT environment, a digital signature will help the system administrator to utilize their private keys to authenticate and validate the devices. Essentially, hash functions are deployed during the signing operations and enciphers the exchanged data using private keys. On the other hand, the verification process involves the usage of hash function while the deciphering procedures involve the public keys. In essence, when the output of the hash function and the data decryption are identical, then the implication is that the digital signature is valid. Otherwise, this particular digital signature is invalid.

Cloud computing: In an IoT environment, a massive amount of data is exchanged across the network. Therefore, the cloud can offer services such as the data storage as well as data analysis. In this regard, IoT benefits from the high processing capabilities of cloud computing and hence artificial intelligence, deep learning and machine learning techniques can be deployed for the prediction of the critical cases of threats and attacks in this environment. In addition, artificial intelligence and machine learning algorithms benefit from the scalability of cloud computing which can enable them to develop reliable and efficient authentication techniques. This enables the IoT environment to prevent malicious entities from invading the network.

Fog edge computing: the fog computing layer is lies between the cloud and the IoT devices. Here, it is utilized to enhance the performance of cloud computing. In so doing, it reduces the communication latency as well as offering availability, scalability and security through the sharing of the data on the cloud.

Identity authentication: To uphold security among the numerous heterogeneous IoT devices and sensors using diverse protocols, standards and scenarios, device fingerprints are deployed. This ensures that the devices can be securely identified so as to protect the sensitive data.

5G networks: Conventionally, the IoT devices and sensors transmit data at low data rates over the cloud. Since numerous devices and sensors are involved, identity and access management can be transmitted at the same time slot. Fortunately, 5G networks can achieve high levels of security and performance and hence can be deployed as the backbone infrastructure to offer high flexibility, fast response times, high data rates, low latencies and high scalability. In addition, 5G can be deployed during the process of authenticating IoT users and devices. Moreover, 5G can help in boosting security in terms of access control, user authentication, key management, device authentication, intrusion detection as well as protection.

Figure 2 illustrates the six concepts that can be deployed to protect the IoT environment from attacks. As shown in Figure 2, these principles include device intelligence using ML algorithms; edge fog processing; device initiated connections; message control, identification, authentication and encryption; and remote control and update of devices.

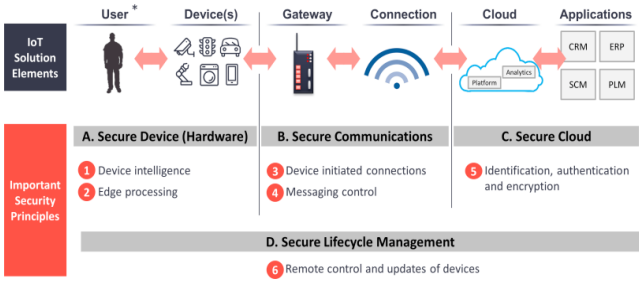

Figure 2. Secure IoT communication architecture

On the other hand, the basic components that are required to secure the IoT environment may include users, devices, gateways, connections, cloud and applications. For instance, user training and awareness, proper device disposal, installation of next generation firewalls at the gateways, and the incorporation of strong authentication protocols during connection establishments can potentially boost security. In addition, the incorporation of security during each step of the application development lifecycle can also go a long towards boosting security.

5. Conclusions

The IoT devices have been widely deployed in numerous application domains. However, privacy, performance and security remain key challenges in this IoT environment. As such, there has been active research on the novel security schemes that can help address these issues. In this paper, an extensive review of these techniques is provided. Based on the findings, it is clear that in as much as some progress has been made in IoT security, a number of challenges still lurk. Consequently, a number of recommendations are provided towards the end of this paper. Future work lies in the actual incorporation of these recommendations in the security solutions so that their effects on security, performance and privacy can be determined.

Conflict of Interest

There is no conflict of interest.

References

[1] Mbarek, B., Ge, M., Pitner, T., 2020. An efficient mutual authentication scheme for internet of things. Internet of things. 9, 100160.

[2] Luo, H., Wen, G., Su, J., et al., 2018. SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system. Wireless Networks. 24(1), 69-78.

[3] Nyangaresi, V.O., 2022. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 3(5), 1-16.

[4] Mamdouh, M., Awad, A.I., Khalaf, A.A., et al., 2021. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. 111, 102491.

[5] Rodrigues, J.J., Segundo, D.B.D.R., Junqueira, H.A., et al., 2018. Enabling technologies for the internet of health things. IEEE Access. 6, 13129-13141.

[6] Hassan, W.H., 2019. Current research on Internet of Things (IoT) security: A survey. Computer networks. 148, 283-294.

[7] Lee, I., 2019. The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. Internet of Things. 7, 100078.

[8] Li, M., Sun, Y., Lu, H., et al., 2019. Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems. IEEE Internet of Things Journal. 7(7), 6266-6278.

[9] Bangui, H., Ge, M., Buhnova, B., 2018. Exploring Big Data Clustering Algorithms for Internet of Things Applications. IoTBDS, Springer. pp. 269-276.

[10] Nyangaresi, V.O., Alsamhi, S.H., 2021. Towards secure traffic signaling in smart grids. 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 196-201). IEEE.

[11] Wang, L., Ali, Y., Nazir, S., et al., 2020. ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods. IEEE Access. 8, 152316-152332.

[12] Zou, S., Xi, J., Wang, S., et al., 2019. Reportcoin: A novel blockchain-based incentive anonymous reporting system. IEEE access. 7, 65544-65559.

[13] El-Hajj, M., Fadlallah, A., Chamoun, M., et al., 2019. A survey of internet of things (IoT) authentication schemes. Sensors. 19(5), 1141.

[14] Kou, L., Shi, Y., Zhang, L., et al., 2019. A lightweight three-factor user authentication protocol for the information perception of IoT. CMC-Computers, Materials & Continua. 58(2), 545-565.

[15] Nyangaresi, V.O., Petrovic, N., 2021. Efficient PUF based authentication protocol for internet of drones. 2021 International Telecommunications Conference (ITC-Egypt) (pp. 1-4). IEEE.

[16] Zhao, B., Zhao, P., Fan, P., 2020. ePUF: A lightweight double identity verification in IoT. Tsinghua Science and Technology. 25(5), 625-635.

[17] Braeken, A., 2018. PUF based authentication protocol for IoT. Symmetry. 10(8), 352.

[18] Xu, H., Ding, J., Li, P., et al., 2018. A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors. 18(3), 760.

[19] Nyangaresi, V.O., Abd-Elnaby, M., Eid, M.M., et al., 2022. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. pp. e4528.

[20] Ding, S., Cao, J., Li, C., et al., 2019. A novel attribute-based access control scheme using blockchain for IoT. IEEE Access. 7, 38431-38441.

[21] Yang, Q., Lu, R., Rong, C., et al., 2019. Guest editorial the convergence of blockchain and IoT: Opportunities, challenges and solutions. IEEE Internet of Things Journal. 6(3), 4556-4560.

[22] Singh, M., 2020. Blockchain technology for data management in Industry 4.0. Blockchain Technology for Industry 4.0 (pp. 59-72). Springer, Singapore.

[23] Jabbar, R., Kharbeche, M., Al-Khalifa, K., et al., 2020. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum. Sensors. 20(14), 3928.

[24] Nyangaresi, V.O., Ogundoyin, S.O., 2021. Certificate Based Authentication Scheme for Smart Homes. 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 202-207). IEEE.

[25] El Beqqal, M., Azizi, M., 2017. Classification of major security attacks against RFID systems. 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS) (pp. 1-6). IEEE.

[26] Khattab, A., Jeddi, Z., Amini, E., et al., 2017. RFID security threats and basic solutions. RFID Security (pp. 27-41). Springer, Cham.

[27] Jia, X., Hu, N., Su, S., et al., 2020. IRBA: an identity-based cross-domain authentication scheme for the internet of things. Electronics. 9(4), 634.

[28] Cheng, X., Zhang, Z., Chen, F., et al., 2019. Secure identity authentication of community medical internet of things. IEEE Access. 7, 115966-115977.

[29] Nyangaresi, V.O., 2021. Provably Secure Protocol for 5G HetNets. 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) (pp. 17-22). IEEE.

[30] Cao, B., Li, Y., Zhang, L., et al., 2019. When Internet of Things meets blockchain: Challenges in distributed consensus. IEEE Network. 33(6), 133-139.

[31] Hammi, M.T., Hammi, B., Bellot, P., et al., 2018.

Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security. 78, 126-142.

[32] Zhang, Y., Ren, F., Wu, A., et al., 2019. Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks. IEEE Access. 7, 114721-114730.

[33] Nyangaresi, V.O., Ahmad, M., Alkhayyat, A., et al., 2022. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. pp. e13126.

[34] Ali, G., Ahmad, N., Cao, Y., et al., 2020. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE Access. 8, 58800-58816.

[35] Jiang, X., Liu, M., Yang, C., et al., 2019. A blockchain-based authentication protocol for WLAN mesh security access. Computers Materials & Continua. 58(1), 45-59.

[36] Jesus, E.F., Chicarino, V.R., De Albuquerque, C.V., et al., 2018. A survey of how to use blockchain to secure internet of things and the stalker attack. Security and Communication Networks.

[37] Dittmann, G., Jelitto, J., 2019. A blockchain proxy for lightweight iot devices. 2019 Crypto valley conference on blockchain technology (CVCBT) (pp. 82-85). IEEE.

[38] Nyangaresi, V.O., 2022. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 15, 100210.

[39] Das, A.K., Wazid, M., Yannam, A.R., et al., 2019. Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access. 7, 55382-55397.

[40] Al-Jaroodi, J., Mohamed, N., Abukhousa, E., 2020. Health 4.0: on the way to realizing the healthcare of the future. IEEE Access. 8, 211189-211210.

[41] Yuan, C., Zhang, W., Wang, X., 2017. EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system. Arabian Journal for Science and Engineering. 42(8), 3275-3287.

[42] Naija, Y., Beroulle, V., Machhout, M., 2018. Security enhancements of a mutual authentication protocol used in a HF full-fledged RFID tag. Journal of Electronic Testing. 34(3), 291-304.

[43] Nyangaresi, V.O., Mohammad, Z., 2023. Session Key Agreement Protocol for Secure D2D Communication. The Fifth International Conference on Safety and Security with IoT (pp. 81-99). Springer, Cham.

[44] Tian, Q., Lin, Y., Guo, X., et al., 2020. An identity authentication method of a MIoT device based on radio frequency (RF) fingerprint technology. Sensors. 20(4), 1213.

[45] Yao, Y., Xingwei, W., Xiaoguang, S., 2011. A cross heterogeneous domain authentication model based on PKI. 2011 Fourth International Symposium on Parallel Architectures, Algorithms and Programming (pp. 325-329). IEEE.

[46] Omar, A.S., Basir, O., 2018. Identity management in IoT networks using blockchain and smart contracts. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 994-1000). IEEE.

[47] Poulter, A.J., Ossont, S.J., Cox, S.J., 2020. Enabling the secure use of Dynamic Identity for the Internet of Things—using the Secure Remote Update Protocol (SRUP). Future Internet. 12(8), 138.

[48] Nyangaresi, V.O., Moundounga, A.R.A., 2021. September. Secure Data Exchange Scheme for Smart Grids. 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 312-316). IEEE.

[49] Shen, J., Gui, Z., Ji, S., et al., 2018. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications. 106, 117-123.

[50] Alzahrani, B.A., Chaudhry, S.A., Barnawi, A., et al., 2020. An anonymous device to device authentication protocol using ECC and self certified public keys usable in Internet of Things based autonomous devices. Electronics. 9(3), 520.

[51] Nyangaresi, V.O., Morsy, M.A., 2021, September. Towards Privacy Preservation in Internet of Drones. 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 306-311). IEEE.

[52] Rathee, P., 2020. Introduction to blockchain and IoT. In Advanced Applications of Blockchain Technology (pp. 1-14). Springer, Singapore.

[53] Wan, Z., Xu, Z., Liu, S., et al., 2020. An internet of things roaming authentication protocol based on heterogeneous fusion mechanism. IEEE Access. 8, 17663-17672.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Implementation of Distributed Control System for Rice Mill Using C#

Hla Myo Tun*

Research Department of Yangon Technological University, Gyogone, Insein PO, 11011, Yangon, Myanmar

ARTICLE INFO

Article history
Received: 14 August 2022
Revised: 28 August 2022
Accepted: 29 August 2022
Published Online: 19 September 2022

Keywords:
Distributed control system
Rice mill
C sharp
Real time simulation
Software development

ABSTRACT

The paper presents the distributed control system for rice mill using C# language. The real-time manufacturing system can be implemented by utilizing the signal from the real time control units that is more operative than other old-fashioned control systems in the extent of modern industrial days. The software-based Distributed Control System (DCS) is novel fashionable than any other conventional control systems in the state-of-the-art manufacturing developments. This research study emphasizes on the implementation of the DCS-based rice mill using visual C#.net. The Industrial Ethernet (IE) is realized between the top level controller for the operator and the controlled station for the remote devices. The model of client-server approach is more appropriate for the automation and manufacturing research purposes. In this study, the computer graphical simulation of the complete control development is depicted in real-time status quo by visual C# language under Visual Studio 2008 software. The parallel ports in the computers of remote terminal level and the master terminal level controllers have been interconnected with port interface coding by visual C# program.

1. Introduction

RICE is the staple food for 100% of the population in Myanmar. It is the major consumed calorie source surrounded by the food grains. With a per capita accessibility of 73.8 kg it convenes 31% of the whole calorie obligation of the population. Myanmar is the world largest producer of rice in the world. Aside from rice milling system, rice bran processing for oil extraction is also a significant agro dispensation action for value accumulation, income and service production [1-7].

Numerous of the rice processing divisions are of the conventional huller type and are unproductive. Up to date rice mills are encompassing elevated capability and are principal concentrated, although incompetent. Miniature contemporary rice mills have been expanded and are obtainable in the market but the need of information is a blockage in its approval by the potential industrialist. The present replica will go a lengthy method in connecting the information break. The overall system block diagram for DCS based rice mill system is illustrated in Figure 1.

*Corresponding Author:
Hla Myo Tun,
Research Department of Yangon Technological University, Gyogone, Insein PO, 11011, Yangon, Myanmar;
Email: hlamyotun@ytu.edu.mm

DOI: https://doi.org/10.30564/jcsr.v4i3.4963

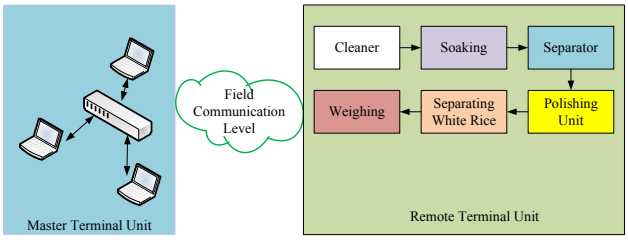

Figure 1. DCS-Based Rice Mill

2. Milling Process

Where the current machinery is touch expensive and manufacturing rate is somewhat towering still the rice generated farther the contemporary machinery has acquired additional order in open marketplace. Foreword of mechanical dryer is a significant adding together in excess of manual sun drying procedure. Here in mechanical drying scheme condensation is being utilized and it is an uninterrupted procedure takes 6 to 7 hours for drying paddy. Benefit is that the rice mills can be operated during rainy condition. Insertion of parboiling with mechanical dryer has been measured as contemporary rice mills in Myanmar. Rest other procedures are ordinary in this region.

When rice is harvested it has a non safe to eat shell or hull neighboring the essential part. At the rice mill, all trails and extra far-off substance are detached from the jagged rice by an assortment of dedicated machinery. Parboiled rice is fashioned using a condensation pressure procedure earlier than milling process. Rice is parboiled in the shell or hull which becomes softer the essence, permitting the exterior starch, fiber and additional parts to comingle.

The water is afterward shattered and the rice is suspiciously condensation dried. The dried parboiled rice is sent throughout machines which eradicate the shell or hull and shine the essence. Brown rice doling out engrosses fleeting the rough rice through defender machines which eradicate the shell or hull, manufacturing brown rice with the bran layers still unharmed around the essence.

Ordinary milled colorless rice is fashioned by eradicating the shell or hull and bran layers. The bran layers are detached by a polishing machine the chafes that grains collectively underneath pressure. The result is a refined white essence [8-12].

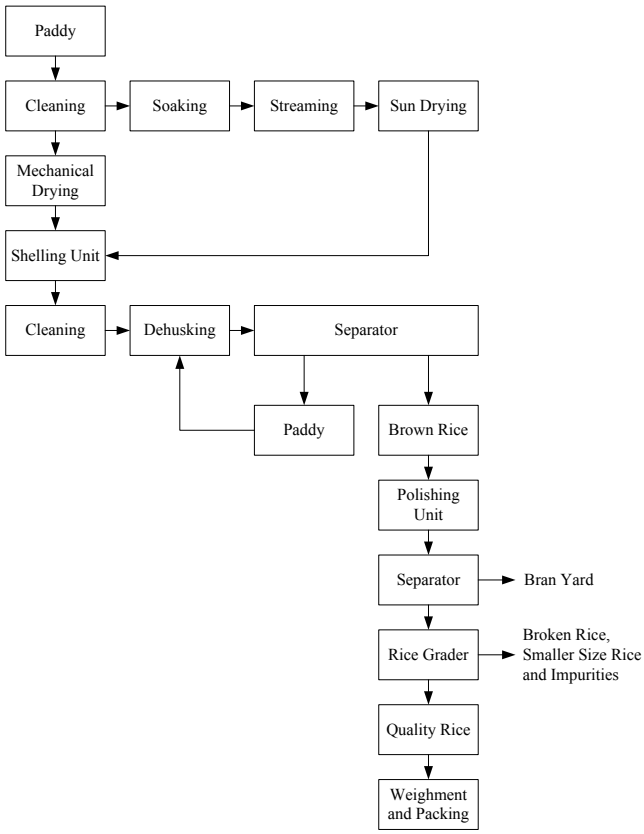

Figure 2. Block Diagram of Raw Rice/Parboiled Rice Processing

3. DCS System for Rice Processing

The DCS composes of a Supervisory Control and Data Acquisition (SCADA) scheme and of front-end schemes. The forename SCADA points out that the functionality is dual: It obtains the information from the front-end modules and it puts forward supervisory control purposes, for instance information dispensation, demonstrating, accumulating and collecting. This facilitates the managing of instructions, communications and agitations. The front-end schemes could be depicted in expressions of campaigns and of Input and Output ports. Front-end schemes can array from straightforward Input and Output devices to sophisticated schemes based on high performance computer which are linked to the SCADA schemes by using industrial communication network. A Real-Time SCADA database includes evidences where the data values are accumulated.

Distributed Control System can be separated into up-

right portions. Such a separation can be activated entirely autonomously from other portions of the DCS and advocates the complete SCADA function to its clients. Two or more separations can be composed of one control province by linking the real-time databases to each other. Apparently, a control province can be made up of a single division additionally. Separations contained by this control province exchange data with both by interpretation and lettering the evidences in the distributed real-time database. With the exception of this database access, there are no additional communication acquaintances recognized between specific divisions of the control scheme. Figure 3 displays a fragment of a control system that includes two divisions coupled to front-end schemes in addition of a SCADA system committed to the supervisory control errands deprived of a through link to the front-ends. These divisions can be energetically set up, e.g. on appeal of the DAQ structure in order to cup tie its segregating [13].

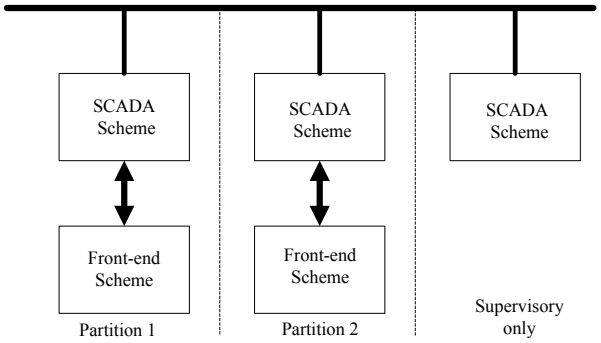

Figure 3. DCS Segregating

4. Software Apparatus of DCS

The similar categories of software apparatus must be utilized for all the dissimilar DCS divisions as revealed in conjunction with the data-flow acquaintances in Figure 4. They are the resulting:

- Systems of disseminated SCADA.
- Control functions using the implementation of SCADA.
- Interfacing to the front-end modules.
- Interfacing to the exterior structures.
- Front-end control purposes for non-SCADA.

A SCADA structure gives a broad variety of services to advance and route a committed purpose for control process. The interfacing to the front-end devices can be realized what's more as innate drivers in the SCADA structures to contact the devices unswervingly associated or utilizing the client–server model. Especially, the consequences of SCADA system have a set of completed device drivers, the OPC user software to link to whichever a manufacturing or a commissioned OPC server and the Application Program Interface (API) library, countenancing an exterior solicitation to contact the run-time database for distributed structures.

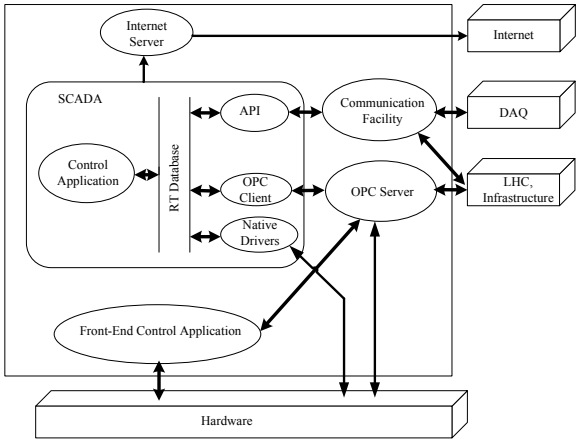

Figure 4. DCS IDE Apparatus

The control function based on SCADA drives most of the purposes essential for the operation of the detector. On the other hand, a convinced set of control functions might be offered wherever appropriate by a control purpose for front-end modules such as a system based on VME with an entrenched computer, or a IDE imitation of a Programmable Logic Controller. The fitting together of the front-end structure to the SCADA systems must be recognized if possible through a committed OPC server. The interfacing to the exterior structures shall be if at all possible established as OPC servers or as customized communication amenities after it is realistic to do so as a consequence of explicit characteristics of the data conversation, as in the occasion of connection with the DAQ structure. Secluded contact to the DCS would be approved through an Internet server in reference to the contact privileges of the diverse categories of handlers.

In the rice production factory, the overall method is accustomed to control SCADA and front-end modules such as DCS architecture. It is revealed in Figure 5. It could manage in a number of control scheme. Nevertheless, most of up-to-the-minute manufacturing system utilize DCS structure as a consequence of system's security and system's reliability. DCS structure includes master terminal unit (MTU) together with server and remote terminal unit (RTU) together with client computers. But it uses only one master station (personal computer). And another plants use PLC controller unit in RTU. The present system can be designed by using PIC microcontroller instead of PLC and other control circuits. The remote terminal unit (RTU) includes interfacing circuit, PIC microcontroller and devices driver control circuit. It uses parallel port communication to connect master station and RTU. The

data from sensors are controlled by the controller circuits and interfacing circuits match the data to understand the computer using parallel port including multiplexers. The motors are operated by PLC controller [14].

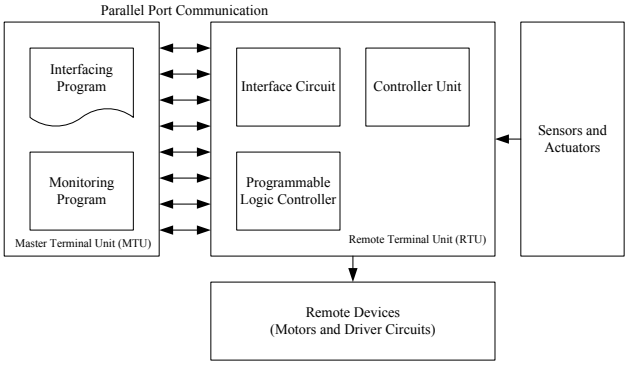

Figure 5. Block Diagram of DCS System for Rice Production Factory

For small factory, it is monitoring system using Visual C#.Net, Visual Basic. It can be designed with real-time monitoring system. So it consists of master station, data acquisition and visualization programs and RTU, signal sensing and supervisory control. DCS software has various types (DiscoNet, ATLAS DCS, Yokogawa DCS, etc.). But it is used own monitoring programs for present plant instead of the DCS software using Visual C#.Net.

This research initiates with an inspection of control systems, and DCS systems specifically. It depicts the diverse components in a DCS system and the diversity of open communications protocols that have been specified. The research then improves a three-tiered model and eventually gives a matrix approach to recitation and defining the features, functions and capabilities of a DCS system.

5. Monitoring and Displaying for DCS System

The basic operation principle of the system is described in following. The monitoring software of main window (personal computer) must run and send appropriate command to the Remote Terminal Unit (RTU) [14,15]. After receiving and checking the command, the data acquisition and processing module (operation window) are processed by the received command. If the command is selected to acquire data from sensors and requested to send acquire data, the operation mode acquire the analog signal input from sensors, process and send the result to output system [16,17].

5.1 Linking Windows System for DCS Process

The process of the DCS could be operated and stopped after central window by controlling of the operator. The main window obliges to accumulate the data from process mode and demonstrate in real-time condition and keep the unruffled information. The graph link is strained in just about 1 second step up until the STOP command is recognized. When the central window program is power cut the data attainment and dispensation is correspondingly shut down all procedure excluding unloading command from the central window. Consequently, the solicitation software can be observed in that windows, the central window of PC and other windows can be linked with other windows in the DCS structure.

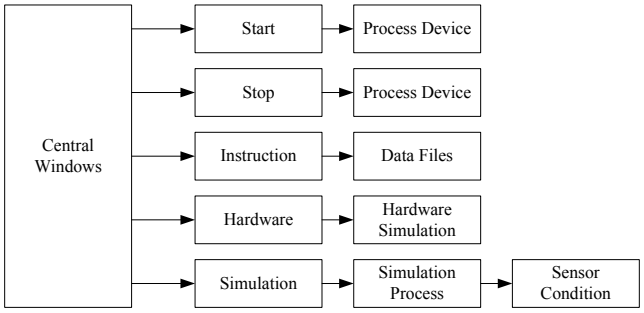

Figure 6. Block Diagram of Linking Window System

5.2 Designing the Program for Central Window

The central window utilizes the Visual C#. Net ration of window solicitation from the Visual Studio 2018 IDE package. It could be considered a window form by utilizing the programming for solicitation information and consumption data by conditional on the procedure from the properties of software items. The modules for controlling purposes are considered on the form by utilizing the toolbox in the package. In addition, the instruction sets of programming language for each of the items are created onto the code viewer by utilizing Visual C# language.

Timer tools are utilized for data timing for interfacing and input and output for the processing of data analysis stage. A timer is utilized to nurture an occurrence at user-defined interludes. Getting the time or setting the time, in millisecond period, is flanked by timer ticks. Window forms timer element has an interval property that stipulates the number of milliseconds that authorization between one timer occurrence and the succeeding. Without the element is incapacitated, an element is intended for a windows forms environs. The signal for read or write purposes of timer carry on to obtain the Tick occurrence at coarsely equivalent to the interval of time. This input and output system galvanizes every time. It utilizes timer tool of (timerIn_Tick) to wristwatch the port structure. The warning sign after timer state is streamed to designated pin of user computers.

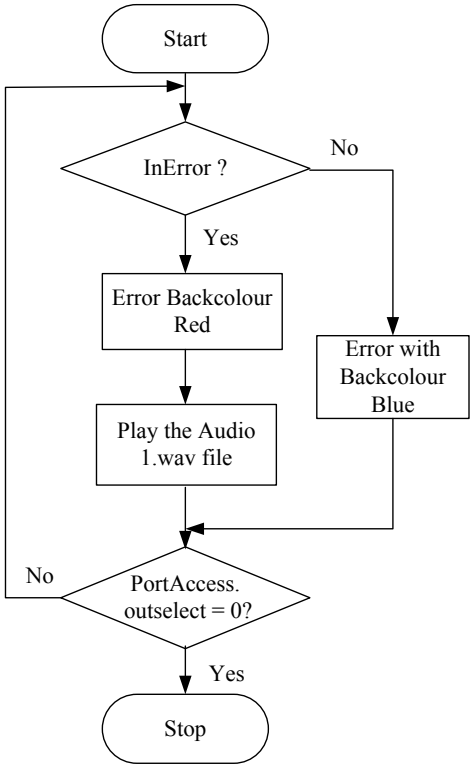

Figure 7. Flowchart of Error System

5.3 Designing the Program for Monitoring with Simulation Window

This window utilizes the monitoring of constituents on the form (SimulationForm). The signal from simulation button for each process is grown to demonstration on the window from timer (timer_In_Tick) of central window. So the location of each of image is put on the form using picture box tool (picName). Next, the text showing the running process and the stopping process displays on the form by using start button on state. This system needs to test how the state of input pin is. So it uses timer tool from window application to display the components. The simulation of running conveyor is used timer tool (timer_Conveyor_Tick) and it is shown in Figure 8. If the input of signal for conveyor (inConveyor) gets from input timer, the displaying of conveyor shows on the form.

The displaying of image for robot gripper is three images of intention for gripping. It utilizes timer tool (timer_Gripper_Tick) to grow indication from the input system. Firstly, the color of work piece sensor put lime. If the signal of input pin (inWorkpiece) is true, it displays the image of full robot gripper (RobotGripper) in the location of image (picGripper) and the red color of work piece sensor on the form. If it is not the above, it is tested true or false for the signal of input pin (inRobotGripper) and if it is true, it displays the image of robot gripper (RobotGripper) in the location of the image (picGripper). If it is not true also the above, it displays the image of normal robot gripper (RobotGripperNormal). The flowchart of simulation for robot gripper control system is shown in Figure 9.

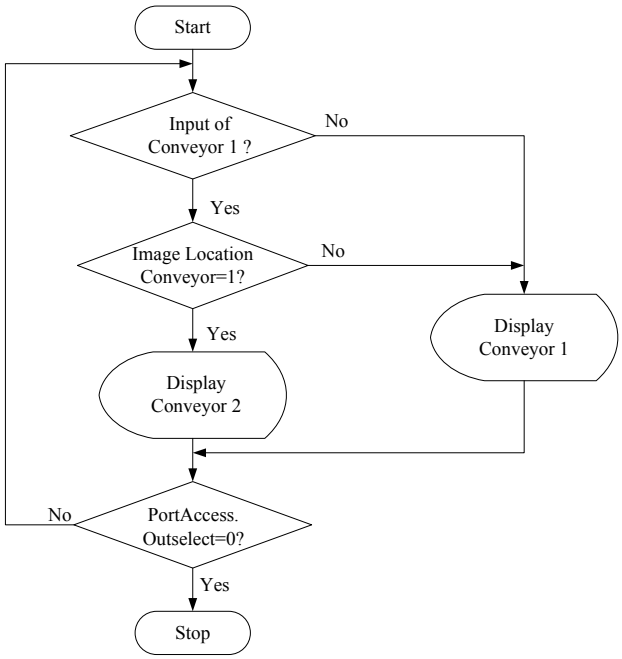

Figure 8. Flowchart of Monitoring for Conveyor

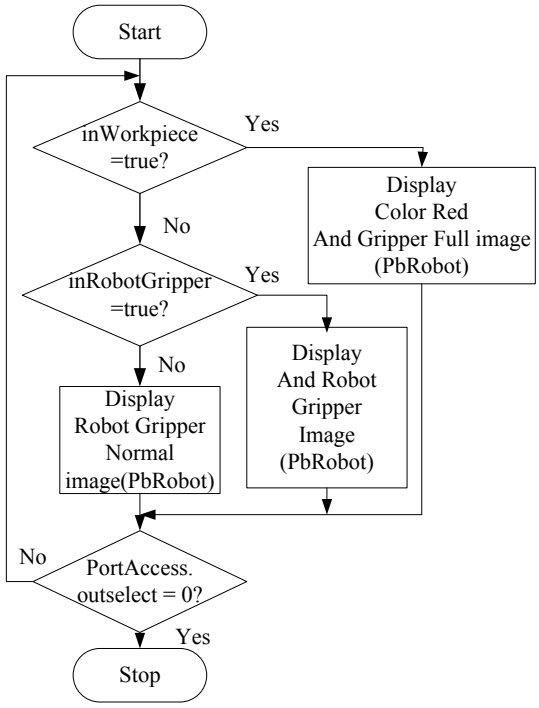

Figure 9. Flowchart of Simulation for Robot Gripper System

6. Simulation Results

6.1 Display Result of Central Window

In this window, it comprises five switches – start switch, stop switch, process switch, simulation switch, instruction switch, hardware switch and exit switch. And it uses two tags appellation together with title and designer appellation, and alarm color scheme utilizing the circumstance of error signal. This window is indispensable for the complete scheme. It comprises the interfacing scheme for the input and output signal from parallel port in addition links with other windows and conducts to the supplementary windows the condition of input and output signal.

The start switches and stop switches are utilized to track and rest the complete scheme which is real-time observing procedure. The simulation switch is used to exhibit the simulation consequence of the procedure. The instruction switch is utilized to prompt the user guide for the scheme. The hardware switch is exploited to confirm the observing of hardware modules by associating with it. The exit switch is utilized to finale the procedure and to walking out the observing scheme by associating with the yes or no message box. It is publicized in Figure 10.

6.2 Display Result of the Simulation Window

In this window, it includes two switches – back switch and sensor switch. This window is a central process to show for entirely procedure. On the form, it is designed with the sample components for the real devices of automation process by utilizing the illustration information of real devices.

It shows the monitoring or moving of each components. It uses input and output signal from central window for procedure of device by utilizing for each signal. It is revealed in Figure 12.

Figure 10. Display Result of the Central Window

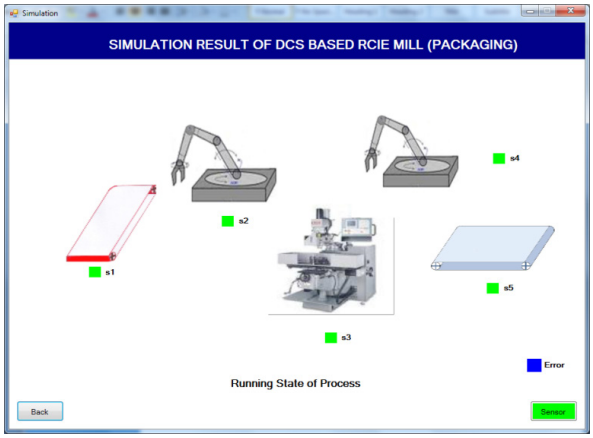

Figure 11. Display Result of Simulation Window

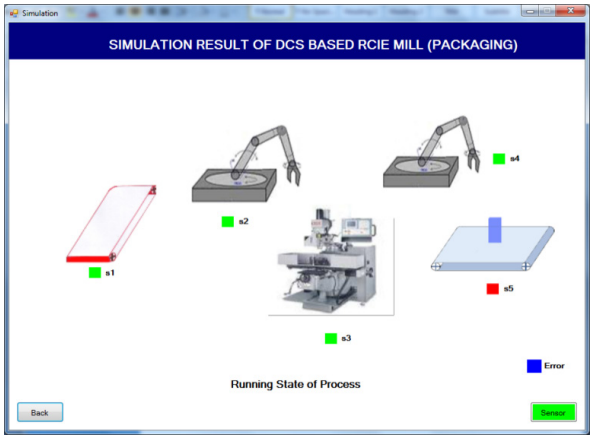

Figure 12. Display Result of Complete Simulation Windows

The back switch is applied to go back the central window like to close the operation window. The sensor switch is used to express the condition of sensors by linking with it. It includes data, hardware, sensor and exit windows. All windows are used by the input signal from each input pins.

6.3 Display Result of the Instruction Window

This window confirms the user guide for the complete scheme how to utilize and what contains it. It is to associate with the central window. It is publicized in Figure 13. If the user desires to go back the central window, the instruction window will be padlocked.

6.4 Display Result of the Visual Hardware Window

This window illustrates the hardware pictures corresponding to the modules of DCS-based structure. If the user impulses the start switch, the complete scheme would track and the arrow pictures would express onto the window form. It associates with central window. The

back switch is utilized to go back the central window that exposed in Figure 14.

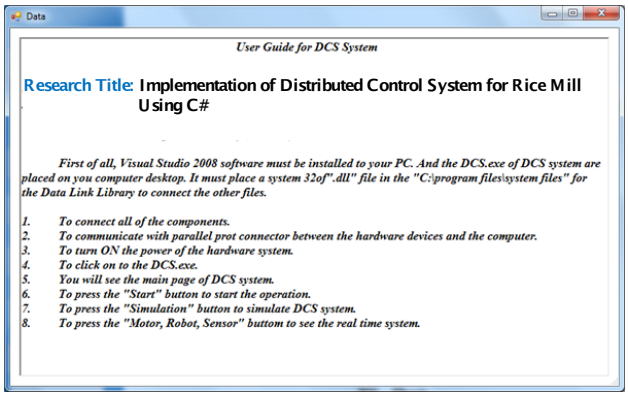

Figure 13. Display Result of Data Window

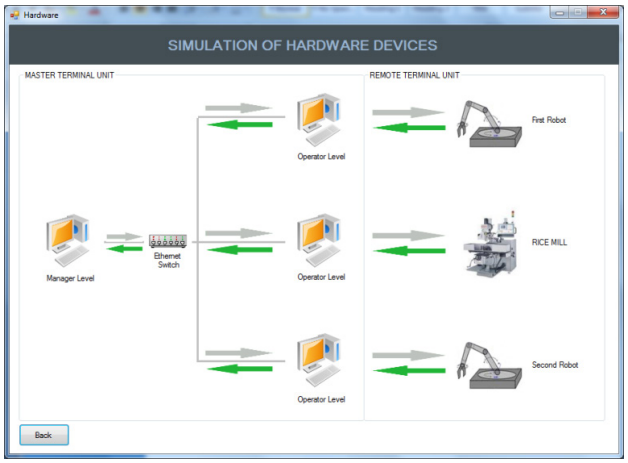

Figure 14. Display Result of Visual Hardware Window

6.5 Display Result of the Sensor Window

This window mentions the conditions of sensor by changing the colors of the running state of the process. It includes three sensors- position sensor for robot (1), position sensor for conveyor, position sensor for robot (2). If the sensors get the signal from input pins, the changing color of sensors will show as red or light green on the form. It links to the simulation window. The back switch is utilized to go back the simulation window. It is exposed in Figure 15.

6.6 Display Result of the Process Window

This window illustrates the procedure of rice production process from paddy. The detailed algorithm has been described in previous chapter. There are at least six processes to produce rice from paddy. They are cleaning, soaking, separating, polishing, separating white rice and weighting. The screenshot result is publicized in Figure 16.

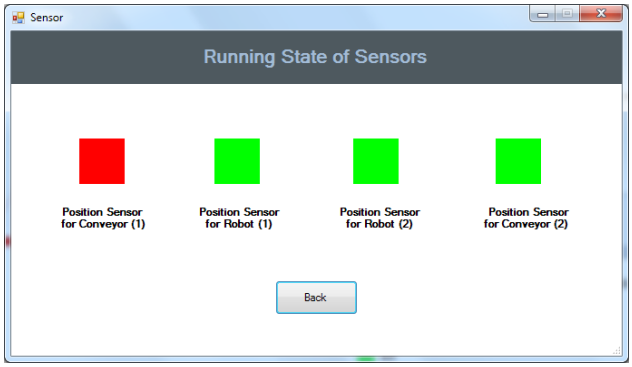

Figure 15. Display Result of the Sensor Window

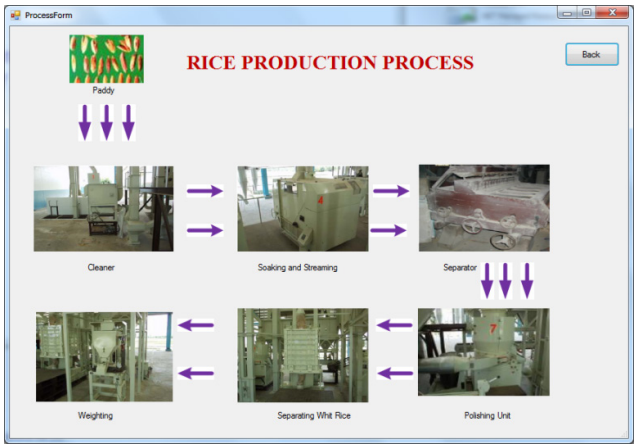

Figure 16. Display Result of the Process Window

6.7 Display Result of the Exit Window

This window displays the decision making for the operator to track or break of the existing circumstance of the complete scheme. It utilizes the message box together with yes or no decision buttons that is if it is the condition of "yes", it will exodus from the scheme or else the process would endure the procedure. It is revealed in Figure 17.

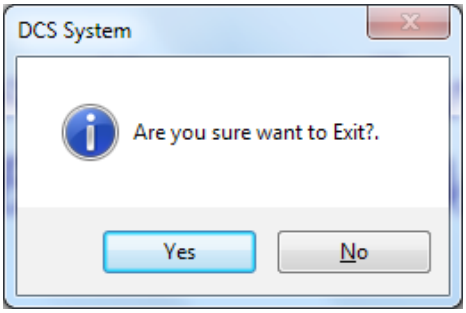

Figure 17. Display outcome of the Exit Window

7. Conclusions

This study certainly intention to advance the governing

hardware devices from all over the place by observing and scheming the complete scheme. This observing scheme can contact with the supplementary progression. This study is established to control the rice mill system by using visual C#. Utilizing this observing control scheme, it is envisioned to develop the process security and process reliability from the MTU. An inexpensive data achievement, dispensation and observing scheme based on the DCS has effectively developed in this research work. Since technologies change quickly, this system is only as good as the ease with which it can be adapted to more complicated system. This research expects technologies of Distributed Control System based rice mill system. It comprises motors, sensors and supplementary hardware devices and applies to control the type of visual basic. net programming like DCS software. And the simulating and monitoring for the industrial automation use own programs without popular DCS software. So it can be used that customers want to desire from their application. It is very suitable price for using this application and has publicized that high performance computers and automatic control can be utilized as a contrivance to upsurge the quality of product and fabrication suppleness. In this research work, rice mill process was used by Visual C#.Net programming for the monitoring of DCS system has been intended and implemented. The communication scheme uses parallel port and circuit that is utilized for interfacing purposes. Hardware devices for this scheme are planned with the trivial emblematic model and confirmed by linking the hardware and computer system, and it could be organized to start and stop with element utilizing observing scheme and can be realized all of state consecutively for this scheme.

Acknowledgment

The author acknowledges many colleagues from automatic control research group of Yangon Technological University.

Conflict of Interest

There is no conflict of interest.

References

[1] Wang, L., Wei, H.Y., 2010. Development of a Distributed Control System for PLC-Based Applications. College of Electronic and Information Engineering, Hebei University.

[2] Bradley, J.C., Millspaugh, A.C., 2009. Programming in Visual C# 2008. Computer and Information Technology, http://www. primisonline.com.

[3] Abolrous, S.A., 2008. Learn C#.

[4] Talamini, G., 1997. Operator Interface Design for Industrial Control. University of Queensland.

[5] Tsourveloudis, N., Ioannidis, S., Valavanis, K., 2006. Fuzzy Surplus Based Distributed Control of Manufacturing Systems, USA, APEM Journal. pp-5-12.

[6] Shivanand, M., Benal, M., Koti, V., 2006. Flexible Manufacturing System.

[7] Cole, E., Krutz, R., Connelly, J., 2005. The Network Security Bible. New York: John Wiley & Sons.

[8] Hugh, J., 2005. Automation Manufacturing Systems with PLCs. Person Education.

[9] Kamen, E.W., 1994. Introduction to Industrial Controls and manufacturing. School of Electrical and Computer Engineering Georgia Institute of Technology.

[10] Beum, H., 2004. Technology Update: Cyber Security Guidance-Interface Technologies. Control Engineering.

[11] Cyberscience Lab report, 2003. Introduction to Networking.

[12] Chen, L., Wang, Y.X., 2002. Design and Implementation of a Web-Based Distributed Control System. Dept. of Electrical & Computer Engineering, Unicersity of Calgary.

[13] Anonymous, 2002. "Distributed Control Systems" Chemical Engineering Department, King Saud University.

[14] Tun, H.M., 2008. Distributed Control System for Vehicle Spare Parts Manufacturing Plant. Real Time Graphical User Interface Monitoring and Networking System.

[15] Tun, H.M., Kyaw, M., Naing, Z.M., 2011. Development of process monitoring system in drilling process using fuzzy rules. International Journal of Systems Assurance. 2, 78-83.
DOI: https://doi.org/10.1007/s13198-011-0054-9

[16] Tun, H.M., Naing, Z.M., Moe, W.K., et al., 2009. Software implementation for distributed monitoring control systems based industrial automation using visual studio. Net. Engineering e-Transaction. 4(1), 47-50.

[17] Tun, H.M., 2008. The future of Visual Basic. Net based simulation for industrial automation: Distributed control systems. AIP Conference Proceedings. American Institute of Physics. 1052(1), 216-219.

BILINGUAL
PUBLISHING CO.
Pioneer of Global Academics Since 1984

Tel.:+65 65881289
E-mail: contact@bilpublishing.com
Website:ojs.bilpublishing.com

2630-5151
03
9 772630 515223