ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 6 , June 2019

Security Improvement on Balise-Based Train Control System

Luyinda Ronald

P. G. Student, School of Information Science and Technology, Southwest Jiaotong University, Chengdu. PR. China

ABSTRACT: Balise remains the most crucial component of the Train Control System (TCS) due to its significant importance to the safety and control of High-Speed Railways (HSR) through its data storage and signal transmissions. Nonetheless, little focus is given to the security of this stored data as well as the signal transmission protocol. This makes it vulnerable to a variety of attacks such as faking of telegram data, impersonation of BTM to collect telegram data, data replay, displacement attack, etc. In this paper, we improve the Balise security by employing the Deoxys-II algorithm which is a nonce-based symmetric AE scheme. It is known for its effective and efficient prevention of faking and replaying of balise telegrams. Deoxys-II security is guaranteed in aspect of its compliance to nonce misuse resistance property of AE. Conducted experiments show the security improvement of the baliseand devoid of any deficiencies of tampering, faking or replaying the telegram again. In addition, real-time test comparison with other existing algorithms depict that our scheme gives the shortest latency from the time spent at the track side encryption of the plaintext to the decryption part at the on-board unit of the train.

KEY WORDS: Balise, Train Control System, Nonce, Deoxys-II algorithm, Telegram Transmission.

I.INTRODUCTION

Being one of the modern means of transportation, the rail system proves to be the most efficient land transport with respect to speed, distance coverage and capacity[1]. As such, the security of balise telegram for safe and reliable train operations, and safeguarding lives aboard a train is undeniably one of the most important aspect that requires topmost consideration With the recent technological advancement in rail systems, Balise happens to bea passive or active transmission unit that uses the magnetic transponder technologyto transmit signals[2]. It ensures the transmission and exchange of the track-to-train information via the Balise-BTM air-gap interface. While the Balise transmits signals to the train,different other essential components of the train control system (TCS) e.g., European Train Control System (ETCS), Chinese Train Control System (CTCS)[3], etc.,communicate mutually for efficient inter-operability. These components include the Lineside Electronic Units (LEUs), Global System for Mobile Communication-Railways (GSM-R), Key Management Centre (KMC), Euroloop, Driver Machine Interface (DMI), Balise Transmission Module (BTM)and Radio Block Centre (RBC).

Basically, Balise is a standalone device that is independently installed on the train track sleeper .It requires no power source in case of a passive balise or is powered by the LEU if it's an active balise, while the BTM is mounted on the train[3]. When the train passes over the balise, radio frequency energy is tele-powered via the BTM. In response, the balise either transmit information (in real time) to the train (uplink) or receives information from the train (downlink). With the provision of enough transmission rate via tele-powering, a passing train can receive a complete telegram at a speed of up to 500 km/h. The LEU supports the balise by storing the pre-stored telegram signal that correspond to the one received by the balise. This telegram is then sent to the active balise for encoding and modulation before finally transferring it to the BTM for onboard usage. After obtaining the telegram, the BTM further decodes the received telegram to a variety of information packets such as geographical position, route data, speed limit etc. hence, creating a ground balise-to-on-board BTM interface which is the balise information transmission system (BITS) that accomplishes the signal transmission process in the open air[4]. The block diagram in Fig.1 depicts the operability and composition of the balise system.

The European Train Control System (ETCS) in ref.[2],[5] came up with a packet type in accordance to the payload in the balise specification which is currently adopted world-wide. This is done in order to ensure interoperability between trains operating in different countries. The type of packet associated with track-to-train telegram includes but not limited to traffic and geographical location information, train operation target information, fixed speed limit, temporary

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

speed limit, driving permit: defining the maximum speed that can be used for a given maximum distance at a given maximum time, track gradient: including track segment length and slope information, associating the relationship data of adjacent balises and so on. This telegram holds crucial information in relation to the train operation and its surroundings. However, this telegram is still vulnerable to a number of possible attacks[6] considering the fact that entire Balise-BTM air-gap transmission interface telegrams are sent in plaintext, thereby lacking security features like any cryptographic protection which could provide the integrity checks or timestamps. Moreover, the physical infrastructure also exhibits a large physical surface attacks since it is typically housed in the open in most locations. Receiving accurate information from the baliseto the on-board BTM is crucial in curbing wrong safety related response. Hence, once the information from the balise is not accurate and lack protection, it is prone to serious vulnerabilities such as tampering and faking telegram data, displacement attack, BTM impersonation to eavesdropping of telegram data, jamming attack, data replay attack, direction reversal attack etc. Compromising any part of the telegram's data would lead to serious consequence including loss of lives and properties. Therefore, it is paramount to secure this information with the best possible security mechanism[7].

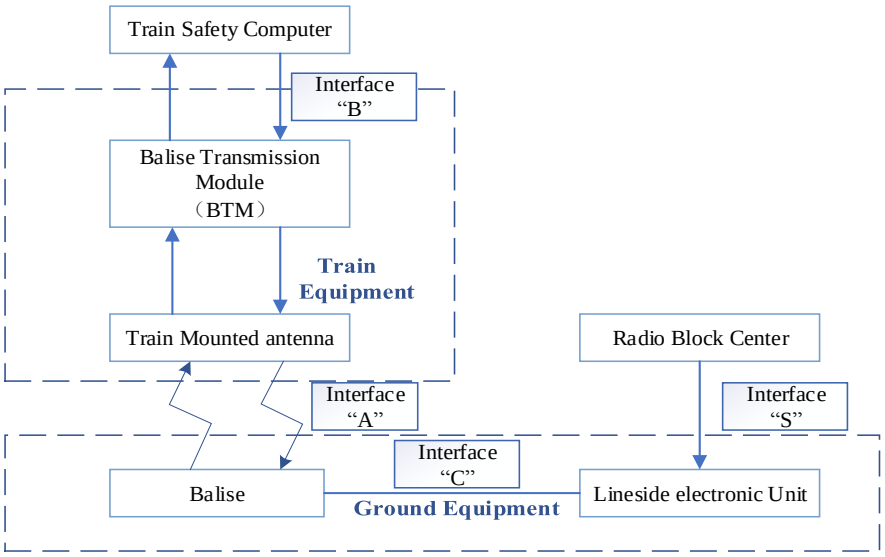

Fig. 1. Block diagram of the Balise system

The remainder of this paper is organised as follows. Section II gives a survey of similar works in the literature and their drawbacks. Section III presents our proposed security improvement using Deoxys-II algorithm as the cryptographic mechanism for balise security enhancement. While Section IV shows the experimental results and analysis as well as the performance comparison between our scheme and other algorithms in the literature. Finally, the conclusion and future works are discussed in Section V.

II. LITERATURE REVIEW

In recent past, researchers have been paying much attention towards the security of balise-to-BTM telegram transmission system considering its enormous vulnerability to malicious attacks due to the fact that telegrams are sent and received in plaintext via wireless communication channel. Also, existing proposed countermeasures shows little to none applicable solutions that are geared towards eliminating or curbing these security problems. In this section, we focus on vital proposals and improve their drawback with strong cryptographic algorithm to secure the Balise-BTM air gap interface transmission and telegram authentication by using authenticated encryption (AE). Some of these existing proposed approaches are given as follows.

Guo et al.[8] Proposes a scheme for protecting the integrity of train balise data. Their scheme is based on three security designs to check data integrity on telegram messages so as to protect the train balise telegram data integrity. They employed AES-CCM an AE for block ciphers and HMAC as cryptographic primitives to ensure integrity, authenticity

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 6 , June 2019

and confidentiality. However, implementing this design allows plaintext to be transmitted from the balise to the BTM, hence invalidating the systems confidentiality. Also, the claim of achieving data integrity checking using HMAC has some shortfalls because when the secret key and plaintext are used as input and applied to HMAC for authentication tag generation, the tag only becomes a new packet that is added to the empty bits.

Harshen et al.[9], proposes a scheme for securing the Balise-BTM using cryptographic random fountains. In their scheme, they transmit telegrams containing random signals in each balise instead of telegrams with fixed information. They also employed a salient feature of the random fountains for challenge response-based interaction between the train and balise for integrity. Nevertheless, their design suggests the use of down-link to authenticate the BTM device, thus, ignoring the up-link. But security improvement of the scheme can only be achieved by incorporating protection in both the up-link and down-link channels.

Wu et al. in Ref. [6], addresses the vulnerabilities on the standard balise air-gap interface, they then carry out vulnerability simulations using the system parameters as specified by the ETCS. In their countermeasures, they proposed the use of down-link channel for delivering telegrams toground devices for attack detection purpose. Therefore, availability of continuous train-to-track channel (if any) provides real time control signal to the train in order to mitigate attacks. However, the system only suggests using the down-link channel for delivering train messages to the ground devices for attack detection. This oppose the latest version of Eurobalise channel linking specification standard ERTMS/ETCS SUBSET-036 which states that "The case that no up-link balises are positioned within the areas where down-link modulation is supposed to be activated"and "Down-link data present at the Interface 'C' is read and elaborated by the LEU, and then passed through to theWayside Signalling Equipment." Therefore, the down-link balise could not perform the authentication processes for the up-link balise. In the proposed scheme we are ignoring the down-link channel and only giving concern to the protection of up-link channel.

Martin et al.[10] derives a probabilistic modelling of the localization task to develop a sensor fusion to fuse the input of Global Navigation Satellite Systems (GNSS) and velocity sensor with digital track map. They use this to model the uncertainties of using a virtual balise as a replacement to infrastructure-based balises. Their localization approach successfully mitigates attacks to the physical balises. Moon et al.[11] also proposes a novel balise telegram decoding scheme through the reduction of position errors which is achieved by minimizing the decoding latency. This scheme enables the decoder to find valid telegrams during single balise passage through the utilization of values from the previous failures. In addition, Wu et al. [12], proposes a scheme that highlighted three major attacks (telegrams jamming, changing localization of transmitting telegrams, changing the total time of transmitting telegrams) that can be crafted to disturb the wireless signals of balise telegrams and ways of mitigating attacks mainly by verifying the received telegrams. Meanwhile, all these schemes face some drawback which has to do with either its vulnerability against a specific attack or the unavailability of authentication protocol during telegram transmission. This paper therefore, employed Deoxys II[13] cryptographic mechanism to ensure the confidentiality, integrity and authenticity of telegram transmission of the balise-to-BTM communication system.

III. SECURITY IMPROVEMENT

Securing the balise system with AE proves to provide simultaneously the required privacy and authenticity to encrypted messages more than the ordinary counterparts; AES-CCM, HMAC and MAC-CRF based-approaches. Our choice of AE focuses on Deoxys-II due to the fact that it was built on tweakable block cipher with two-pass data processing procedures, where the authentication tag and plaintext encryption tweak tag are generated by each respective pass. Some of the underlying features incorporated with Deoxys-II include efficiency for small messages, nonce misuse resistance, security proofs, simplicity, parallelization and resistant to side-channel attacks. Its integration with the balise-to-BTM ensures transmitted telegrams are authenticated, encrypted and verified. Hence, countering the available schemes where data is transmitted in plaintext and the transmission at both balise side and on-board devices are prone to attacks. Deoxys-II also has the ability of transmitting Associated Data (AD) alongside other encrypted data simultaneously. Due to its nonce misuse detection capability, it can easily counter attacks such as telegram malicious tampering, faking balise telegram data, balise displacement, data replay, as well as insertion and deletion attacks. Our preference to use Deoxys-II is due to the security strength it possesses under all the factors suitable to improve the security of balise-to-BTM communication channel of the balise-based transmission system.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

A. Improvement on data classification

In order to conform to the set of balise encoding and decoding processes, we first format our balise user data structure, data packet and payload data in accordance with the ERTMS/ETCS packets formatting. With the purpose of selecting the balise_ID, we format the user data packets responsible for the track-to-train communication. Then we identify the corresponding dataset and finally meet the set data format requirement. The considered data packets include the following. Packet number 2 for system version order, packet number 65 for temporary speed restriction, packet number 66 for temporary speed restriction revocation, packet number 79 for geographical position information, packet number 145 for inhibition of balise group message inconsistency reaction and packet number 254 for default balise loop or RIU information.

Regarding the payload telegram formatting in Ref. [2], a long telegram of 1023 bits was transmitted to the train on-board unit by the balise. We also have 913 bits of shaped data of which 830 bits are for the converted payload. Others include the control bits (3 bits), scrambling bits (12 bits), extra shaping bits (10 bits), and the checksum bits (85 bits). The payload data structure in the telegram has data packet 79 for the geographical position, data packet 65 which is the temporary speed restrictions, and data packet 66 for temporary speed restriction revocation[14], [15]. We also have 50 bits as our frame flag, 772 bits as user data package and 8 bits as end bit. From the 830 bits of the shaped data, there are 264 bits for both the geographical position and speed restriction and 566 bits as empty bits. All these representations can be seen in the telegram payload data structure as depicted in Fig. 2.

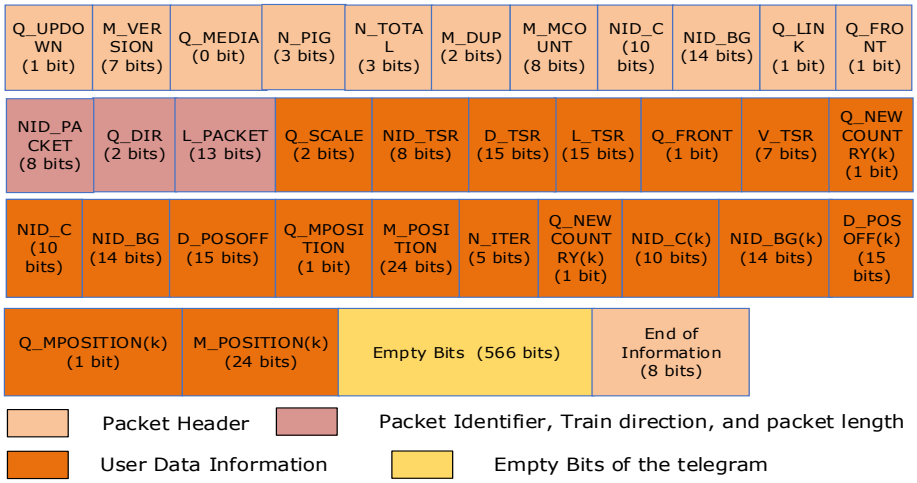

Fig. 2. Telegram payload data structure

B. Authentication key, Tag, and Nonce Generation

In addition, the authentication key, nonce and tag were all generated with the balise-to-train communication security in mind. The generated session secret key for the balise K_{BN} has a key bit length of 128 bits. We use the master key M_K generated and verified offline by the key management centre as the trusted keys controller, pre-assigned to each train using the track and the balise number BN={ BN_0, BN_1, BN_2, …. , BN_{n-1}, BN_n}, where, n is the balise number in balise group, to generate session keys K_{BN} for each balise in the group. The nonce as an arbitrary number used only once in a cryptographic communication,is generated in a counter number produced by the 120 bit counter. This served the purpose that each time the balise is activated, Deoxys-II $E: Key \times \{0,1\}^n \rightarrow \{0,1\}^n$, encryption routine chooses the Initial Vector (counter) $N = C_0$ internally at random and incremented then by counter +1in order to achieve semantic security[16]–[18]. And finally, the authentication tag T is generated by inputting the balise secret key K_{BN} of length 128 bits, the counter (Nonce) N of length 120 bits, association data A, and the plaintext (message) M of block size length 128 bits into the Deoxys-II authenticated encryption algorithm. Hence, outputting two-bit strings ciphertext C and authentication tag T, each of 128 bits block size length.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

C. Transmission of Secure Telegram

In order to secure the telegram transmission process, we began by formatting the ciphertext C and Tag T. Here, the generated tag is put in the original message payload in the empty bits section whereas, the ciphertext after appending it with the balise number, nonce, and associated data, is also put in payload empty bits and the authentication tag. Together this is appended and embedded in the balise original telegram payload data as a packet which will subsequently be sent to the train via the triggered tele-powering process.

Next, to ensure authenticity of the transmitted telegram, the confidential data of the telegram is encrypted while embedding it in the balise. This guarantee that the adversary doesn't get access to the transmitted information through eavesdropping. Hence, the on-board BTM Deoxys-II function decrypts and authenticates the cyclically received message to guarantee that there are no errors during transmission, no tampering, no any replays, no insertions or deletions attacks before sending it to the vital computer.

To begin with encoding, let$E$denote the encryption part which takes four variables as input; a variable-length plaintext M (with $m = |M|$) with a block size length of 128 bits, a variable-length associated data A (with $a = |A|$) of any length in blocks of 128 bits , a fixed-length counter number (Nonce) N of 120 bits and a k-bit key K_{BN} of length 128 bits to represent the key in the authenticated encryption scheme. It outputs am-bit ciphertext C and a T-bit tag of length 128 bits each, encryption function is denoted by $E_{K_{BN}}(N, A, M) = (C, tag)$. While the decryption part D is done on the $M^{'}$ variables as inputs, which includes; a variable-length ciphertext C, a τ -bit tag tag authenticated by the entire message $M^{'}$, a variable-length associated data$A$, a fixed-length encoded as 120 bits random counter number N and a k-bit key K_{BN}. The K_{BN},

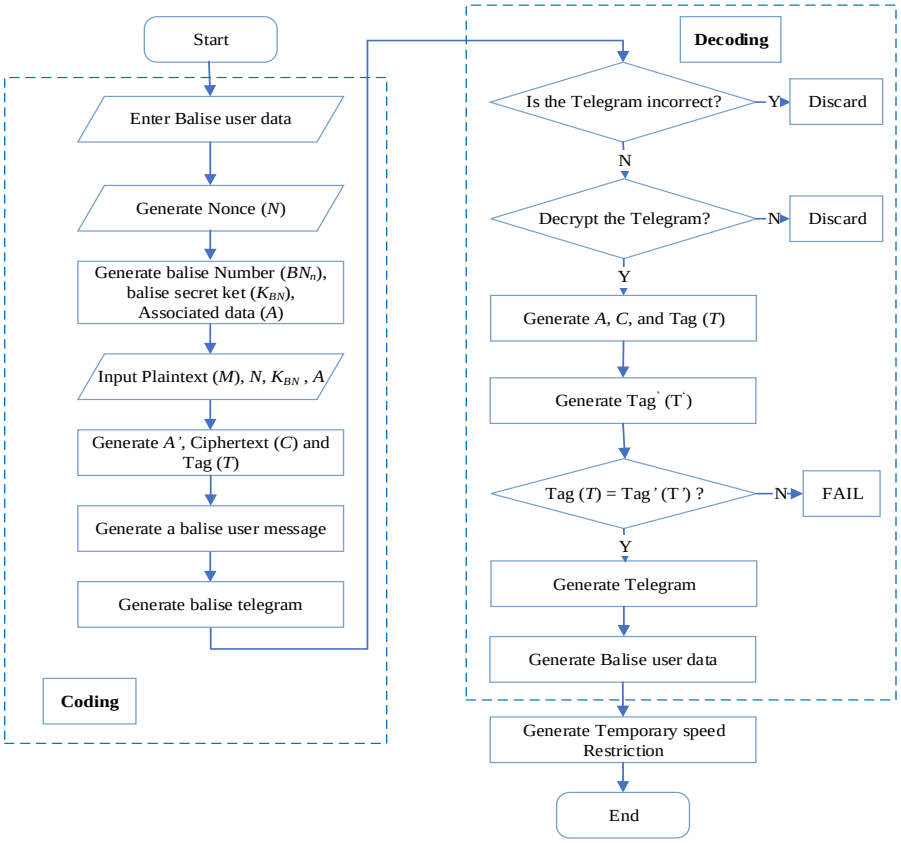

Fig. 3. Deoxys-II Balise encryption and decryption system flowchart

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

is computed after the on-board Deoxys-II function first applies the 128 bits pre-assigned Master KeyM_K to the balise number appended as associated data to calculate the balise secret key K_{BN}. After computing the K_{BN}, the function can proceed to decipher the encrypted packets application information, Nonce, and authentication tag. Upon a successful deciphering, the newly computed tag tag is compared with the transmitted tag$'$, and the algorithm outputs either an error string $\perp$ to signify that the verification failed, or a m-bit string where, $M = \boldsymbol{D}_{K_{BN}}(N, A, C, tag\ T)$ when the tag is valid. Fig.3 illustrates a flowchart depicting the Deoxys-II encryption and decryption functionality on the telegram.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

At this stage, two experiments were conducted in order to validate the correctness and efficiency of using Deoxys-II for security improvement.
It is noted that all test were carried out on provided data packet in accordance to the specification requirement of balise encoding and decoding as illustrated in section III. Also, experimentation of the Deoxys-II algorithm was performed on Windows 10, 64-bit Operating System (OS) portable computer (PC) with C++ programming environment and Visual studio platform as the software components and a RAM of 8.00 gigabyte running on Intel(R) Pentium CPU N3540 at 2.16 GHz.

A. Correctness Results

The first experiment is the encoding and decoding test which was performed on the geographical position referencing information data packet so as to ensure the correctness of the tested Deoxys-II algorithm. While performing this test, the balise secret key of bit length 128 bits and a nonce of 120 bits as its length was generated. Deoxys-II successfully encrypted the packet after various checking if there might be some errors from the encryption side, or errors that might have occurred while appending the AD to the ciphertext, or during the nonce, secret key or authentication tag generation, and decrypted the telegram successfully to output the transmitted packet data. Thus, signifying that the algorithm is correct and authentic thereby, countering balise vulnerable attacks like the forgery and replay attacks. Findings support our argument for the opposite would be outputing FAIL to show that the data was either tampered with, or had error while going through the shaping process. This guarantees that regardless of what packet message is transmitted through the algorithm, it is free of data manipulation, forgery, deletion or insertion, and can't be replayed. Therefore, we have achieved maximum security as our paramount goal to counter such attacks. Table 1 below shows the analysis of the Deoxys-II test packet correctness test.

Table 1. Deoxys-II test packet correctness test

Test Packet	Category	
Plaintext input	AD_1	910E 007F FFFF 8BC1 3700 0000 0000 0000
	AD_2	0000 0000 0000 0000 0000 0000 0000 0000
	M_1	6FFF FFC0 0008 0000 0FC0 07FF E000 1000
	M_2	0010 0000 0000 0000 0000 0000 0000 0000
Nonce	N	06F73 B8B78 6F9FA C54DB 9A021 EA49F
Generated Tag	T	D525 C50E EDAA A556 17A7 C304 8F1E 0A2F
Ciphertext Output	C_1	A589 8E4E 9398 17B6 84C8 1A2E D593 321A
	C_2	3C85 8246 3943 433E 50EE 5EFF 07F1 9CE5
Successful Output	M'_1	
	M'_2	

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

B. Real-Time Results and analysis

In the second experiment, the Deoxys-II algorithm real-time evaluation was taken through running the test data packet over 1000 cycles for both the encryption and decryption sides observing the time spent to compute the message at each side of encryption and decryption.The time unit is recorded in milliseconds (ms) and all the test results are all averaged by the algorithm after running over 1000 cycles. Table 2 shows Deoxys-II test packet real-time test analysis. From this real-time test analysis result, it can clearly be seen that the efficiency of the Deoxys-II algorithm operation on the encryption and decryption of a telegram in such a very short period of time as extimated to be 0.333684 milliseconds on a long message which means it would be even much less if it was a short message.

Table 2. Deoxys-II Test packet real-time analysis

Testing Operation	Time (ms)
Encryption (Balise side)	0.168089
Decryption (BTM side)	0.165595

C. Real-time test comparison

To further elaborate the efficiency of Deoxys-II over other related cryptographic algorithms, we compare the packet real-time test results on all selected algorithms as cited in the work of Guo et al.[8] and Harshan et al.[9]. To make the comparisons as fair as possible, the original parameters and evaluation metrics of the employed algorithms, and results were also adopted here. Even where we made use of a way longer bits of 128 bit length of Deoxys-II unlike ordinary MACs, this essentially means longer time to be taken to break the tag, we still maintain their shorter bits of 16byte tag for BTM on AES-CCM (ciphertext), 16 byte tag for BTM on AES-CCM (plaintext), 16 byte in length for BTM-HMAC (MD5), 20 bytes in length for BTM-HMAC (SHA1), 32 bytes in length for BTM-HMAC (SHA256), 48 bytes in length for BTM-HMAC (SHA384), 64 bytes in length for BTM-HMAC (SHA512) and 128 bits for BTM-MAC (CRF). During their evaluations, test packets on the time spent for both encryption and decryption is depicted; on HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, MAC-CRF, AES-CCM,were0.9216, 1.155, 1.291, 1.167, 1.575, 4.411, and 4.476milliseconds respectively and our proposed Deoxys-II real-time test result is 0.334 milliseconds as Table 3 summarizes the real-time test efficiency comparison among different algorithms. It can clearly be seen that our algorithm has the shortest period of time spent, AES-CCM with the longest time of 4.476 milliseconds, followed by MAC-CRF which ended up spending 4.411 milliseconds. Overall, our scheme has the best performance efficiency while AES-CCM in the category of authenticated encryption happens to have the least efficiency in terms of real-time test. Nevertheless, compared to the time required for the trackside communication-based train control (CBTC) equipment reaction of between 0.07 seconds to 1 second (0.07 – 1 second), and on-board CBTC equipment reaction time of 0.07 seconds to 0.75 seconds (0.07 – 0.75 seconds)[19], Deoxys-II is too far more efficient than all the other algorithms with that time range.

Table 3. Real-time test efficiency comparison among different algorithms

	HMAC					MAC	AE	
Algorithms	MD5	SHA1	SHA256	SHA384	SHA512	CRF	AES-CCM	Deoxys-II (Proposed)
Time taken	0.9216	1.155	1.291	1.617	1.575	4.411	4.476	0.334

V.CONCLUSION AND FUTURE WORK

In this study, we propose to improve the security of Balise-based train control system using Deoxys-II cryptographic mechanism, we implement it for security improvement of the balise-BTM TCS communication channel to counter

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 6 , June 2019

cryptographic related attacks. The algorithm has proved its efficiency and correctness in its operations. The tested packets results have clearly indicated its correctness to guard against attacks and its real-time efficiency shows effectiveness in implementing tasks at the shortest possible time. Comparison with other related algorithms show that our scheme has better performance efficiency than the counterpart algorithms in real-time test analysis. Future works include, incorporating Deoxys-II algorithm as an advanced cryptographic mechanism in the communication-based train control (CBTC) system for perfecting train localization, safety, and reliability.

REFERENCES

[1] M. Palumbo, M. Ruscigno, and J. Scalise, "The ERTMS/ETCS signalling system," *railwaysignalling.eu*, vol. 6, pp. 1–60, 2014.
[2] UNISIG, "FFFIS for Eurobalise Ref. SUBSET-036," *ERTMS/ETCS*, no. 3.0.0, 2012.
[3] B. Ning, T. Tang, K. Qiu, C. Gao, and Q. Wang, "CTCS—Chinese Train Control System," *WIT Trans. Built Environ.*, vol. 74, May 2004.
[4] L. Zhao and Y. Jiang, "Modeling and Optimization research for dynamic transmission process of Balise tele-powering signal in high-speed Railways," *Prog. Electromagn. Res.*, vol. 140, pp. 563–588, 2014.
[5] E. Union, "Call for 'Study on Cyber-Security in Land Transport, Developing Reporting Guidelines, Ranking Possible Attack Scenarios and Adapting Existing Risk Assessment Methodologies,'" 2013.
[6] Y. Wu, J. Weng, Z. Tang, X. Li, and R. H. Deng, "Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 4, pp. 814–823, 2017.
[7] Z. Wang and L. Jia, *The theory and method of design and optimization for Railway Intelligent Transportation Systems (RITS)*. Sharjah, UAE: Bentham Science, 2011.
[8] H. Guo, J. Z. Wei Sim, B. Veeravalli, and J. Lu, "Protecting Train Balise Telegram Data Integrity," *IEEE Conf. Intell. Transp. Syst. Proceedings, ITSC*, vol. 2018-Novem, pp. 806–811, 2018.
[9] J. Harshan, S. Y. Chang, S. Kang, and Y. C. Hu, "Securing balise-based train control systems using cryptographic random fountains," *2017 IEEE Conf. Commun. Netw. Secur. CNS 2017*, vol. 2017-Janua, pp. 405–410, 2017.
[10] M. Lauer and D. Stein, "A Train Localization Algorithm for Train Protection Systems of the Future," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 970–979, 2015.
[11] S. Moon, S. Park, J. H. Lee, and Y. Lee, "Rapid Balise Telegram Decoder with Modified LFSR Architecture for Train Protection Systems," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 66, no. 2, pp. 272–276, 2019.
[12] Y. Wu, Z. Wei, J. Weng, and R. H. Deng, "Position Manipulation Attacks to Balise-Based Train Automatic Stop Control," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5287–5301, 2018.
[13] J. Jean, I. Nikolic, T. Peyrin, and Y. Seurin, "Deoxys v1.41, 2016," *Submitt. to CAESAR Compet. http//competitions.cr.yp.to/ caesar-submissions.html*.
[14] UNISIG, "System Requirements Specification- ERTMS/ETCS languages SUBSET-026-7," *ERTMS/ETCS*, no. 3.4.0, pp. 1–86, 2014.
[15] UNISIG, "System Requirements Specification- Messages SUBSET-026-8," *ERTMS/ETCS*, no. 3.4.0, pp. 1–33, 2014.
[16] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, pp. 270–299, 1984.
[17] P. Rogaway, "Nonce-Based Symmetric Encryption," *Int. Work. fast Softw. encryption (FSE), Lect. Notes Comput. Sci.*, vol. 3017, pp. 348–358, 2004.
[18] P. Rogaway and T. Shrimpton, "A Provable-Security Treatment of the Key-Wrap Problem," *Adv. Cryptol. - EUROCRYPT 2006, 25th Annu. Int. Conf. Theory Appl. Cryptogr. Tech.*, vol. 4004, pp. 373–390, 2006.
[19] H. W. Lim, W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and J. Zhou, "Data Integrity Threats and Countermeasures in Railway Spot Transmission Systems," pp. 1–14, 2017.

AUTHOR'S BIOGRAPHY

Ronald Luyindawas awarded a Bachelor of Science Degree in Computer Science from Nkumba University, Entebbe, Uganda, in 2014 and currently a Postgraduate student in Information Security, Southwest Jiaotong University, Chengdu, Sichuan Province, People'sRepublic of China, in 2019.

He is Information and Technology Officer working in the Public Service of the Republic of Uganda.

His research interests include Cryptanalysis, Network Security, Information Security, and Public Safety & Security.