Optimized Authentication for Wireless Body Area Network

A. S. AL-Khaleefa [1], M. R. Ahmad[1], R.C. Muniyandi[2], R. F. Malik[3] and A. A. M. Isa[1]
[1]*BBNET, Centre for Telecommunication Research and Innovation (CeTRI), Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer (FKEKK), Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka, Malaysia.*
[2]*Research Center for Software Technology and Management, Faculty of Technology and Information Science, Universiti Kebangsaan Malaysia, Malaysia.*
[3]*Faculty of Computer Science, Universitas Sriwijaya (UNSRI), Inderalaya, Sumatera Selatan, Indonesia.*
riduan@utem.edu.my

***Abstract*—In this paper, we propose a novel technique for determining the Cyclic Redundancy Code (CRC) polynomials with the help of a heuristic search (Genetic Algorithms) for Wireless Body Area Networks (WBAN). We apply the resulting CRCs and an encryption technique for improving the error detection in the WBANs. Thereafter, we compare the resulting polynomials, with or without the encryption headers with the benchmark polynomial. Since the Ad-hoc On-demand Distance Vector (AODV) routing protocol is practical in WBAN, we integrated this protocol with the proposed technique for evaluating its performance. The main objective is to improve the error detection rate, which then improves the Packet Delivery Ratio (PDR) along with the network resource usage efficiency. The results indicated that this method is very successful, as it improved the PDR while decreasing the end-to-end (E2E) delay. The overhead is seen to increase because of the use of a novel control message. Also, the energy consumption increased due to the error messages was resent and due to the retransmission of the data packets. All these increased values are acceptable and led to an 80% increase in the PDR values for the stand-up scenario and a 23% increase for the hand waving scenario.**

***Index Terms*— Cyclic redundancy check, Genetic algorithm, Wireless body area network.**

I. INTRODUCTION

The Mobile Ad Hoc Network (MANET) represents a set of autonomous nodes that are interconnected with one another without any central administration [1]. All the nodes in the network consist of a restricted transmission range and can send or receive data packets via a multi-hop process. Thus, every node in the MANET acts as a host or router.

One application of the sensor network technology involves monitoring of human health [2]. Wireless Body Area Network (WBAN) is a form of the MANET technology wherein all the nodes comprise of small wireless sensors that can be worn or planted [3] on the body [2]. The sensors comprise of 4 units, i.e., capture, processing, transmission, and energy control units [3] [4]. The data is transmitted as packets, and a communication is established with the external base station through the sink nodes. A routing protocol establishes this routing of the data packets between the nodes and also determines the routes for data transmission through the sensor nodes so that they reach their destination [5]. One such routing protocol includes the Ad-hoc On-demand Distance Vector (AODV).

The WBAN consists of sensors and helps in keeping track of important signs, provides real-time feedback regarding the patient diagnostic processes [6] and can report the patient recovery progress because of illnesses or any surgical procedures [2]. Though WBAN has many benefits and is very popular in the healthcare sector, some limitations are observed with regards to preserving the data confidentiality or patient privacy [7], and the data integrity [8]. All these limitations arise due to its wireless nature.

The signals sent between the sender and the receiver nodes get disturbed due to dynamic distances, noises, non-linear line-of-sight, human anatomy, shadowing effect(s), and a fading phenomenon [9]. These factors corrupt the data packets, which need to be re-sent from their originating nodes, thereby decreasing the network PDR. As a result, many network resources are employed for resending the copies of the data packets [10].

One way to reduce the number of the corrupted data messages involves their detection at their destination. Also, errors during data transmission are detected using the Cyclic Redundancy Checks (CRC), as their efficiency depends on the polynomials used. The standard CRC implementation techniques are not very efficient; hence, some new implementation techniques have to be used, which are efficient in some aspects [11].

Better PDR indicates an efficient use of the network resources since the relay nodes prevent the transmission of data packets with compromised integrity. Thereafter, a notification is sent to the source node, which states that a corrupted data packet was transmitted. Once this notification is received, the source node begins a new transmission procedure and the message is resent. This decreases the distance travelled by the data packet before it is detected as corrupted, thus, improving the network efficiency.

II. RELATED WORK

The WBAN system is infiltrated by interfering with the routing protocol. In [1], different attacks occurring on the routing protocols along with attempts made for protecting the network have been discussed. In [12], the researchers proposed a novel optimised security scheme (which included the enhanced random key management), which comprised of the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, which was based on the symmetric-key functions and simultaneously preserved the protocol core. This protocol employed the Random Pair-wise Keys (RPK) as its symmetric key system. This modified protocol displayed a mildly higher overhead value; however, due to its security

benefits; it was seen to be much better than the primary protocol.

In another study [13], the researchers discussed the Disruption-Tolerant Networks (DTNs) and described a cost-effective method for transferring the data through many unpredictable or irregular connections. The researchers also emphasized that the nodes could transmit the data packets despite their identities, but it could be subjected to many attacks like Denial-of-Service (DoS), black holes or wormholes. Hence, they suggested a Secure REputation-based Dynamic (SReD) window scheme, which relieved some of the routing layer attacks and also showed a good performance in a general setting. The SReD system showed the following characteristic features: this system was (1) localized, (2) link-state-based, and (3) supported a multi-path routing [10]. This scheme considered the 'trust index' for every node and its adjacent node, designed an algorithm for the probability, and thereafter, switched between a few of the initial nodes.

Moreover, [14] proposed novel architectural design for improving the security of the wireless sensor networks, which consisted of the WBAN, and was known as the "Wireless Sensor Network Security Framework (WSNSF) architecture". This system provided a secure routing as it used the dynamic key cryptography. Many different protocols consist of numerous other mechanisms, and hence, research is aimed towards protecting these protocols from specific attacks, for instance, the Probabilistic Routing Protocol which used the History of Encounters and Transitivity (PRoPHET).

Another queuing mechanism was proposed by [15], based on the probability of restricting or limiting the flooding attacks. In another study, [16] proposed a novel Trust-based Security Protocol (TSP) which protected the system against the black-hole attacks, while [17] developed and investigated a DoS-resistant data transmission system for the WSNs.

A secure data transmission can be achieved based on its geo-location. In one study [18] proposed a novel framework that used the geo-location bound secret keys for securing the WSN. Here, every node was seen to store the keys depending on their position. Hence, the nodes only received the packets from the other authorized nodes as the primary nodes were aware of the origin of the data packets.

To the best of our knowledge, no research study has addressed the problems related to data integrity and used a CRC perspective for improving the data transmission in a WBAN system.

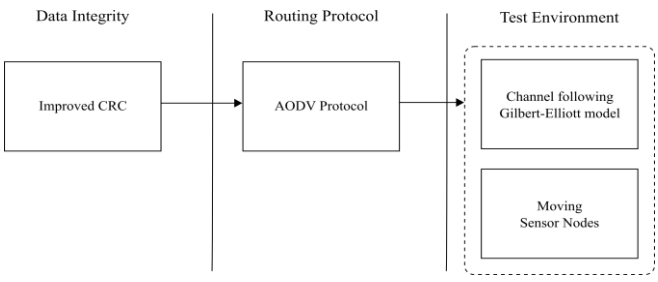

Figure 1: Description of methodology process

III. METHODOLOGY

The main objective of this study is to develop a novel authentication method for the WBANs, for maintaining a minimal number of undetected error data packets. Hence, we have introduced an AODV routing protocol which uses the improved CRC protocol. Thereafter, we evaluated this proposed system consisting of channel parameters which were based on the Gilbert-Elliott model.

This Gilbert-Elliott model was initially developed by [19] and [20] and consisted of a varying binary symmetric channel. The crossover probabilities in this model were determined by the current state of the discrete-time, stationary binary Markov processes. These states were appropriately designated as G indicating "good" or B indicating "bad". As this model was based on the Markov process, it consisted of a memory that depended on the variable probabilities of the states [21]. Hence, the WBAN sensor nodes could communicate with one another via a channel based on the Gilbert-Elliott model. Figure 1 presents a visual summary of the technique. The subsequent subsections describe the AODV routing, enhanced CRC polynomial, and the simulation model used in this study.

A. Ad-hoc On-demand Distance Routing (AODV)

The routing of the data packets between the nodes within the ad-hoc network can be achieved by using routing protocols that determine the routes for transmitting the data packets through the sensor nodes so that they reached their destination. One such routing protocol is known as the AODV. The Internet Engineering Task Force (IETF) stated that the AODV was used by the mobile nodes with an ad hoc network. This protocol offered a rapid adaptation to the dynamic link conditions, required a lower network utilisation, low processing, and memory overhead, and helped the nodes in determining the unicast routes to their destination within an ad hoc network. Ad-hoc On-demand Distance Vector protocol used the destination sequence numbers for ensuring the loop freedom constantly (even during the anomalous delivery of the routing control messages), and for avoiding the problems (like the 'counting to infinity') which were related to the conventional distance vector protocols [22] [23].

B. Improved CRC Polynomial

The CRC codes are a very popular and recognisable form of the data integrity mechanism and are used in the industries for digital communication. Often, they are the primary line of defence and can detect the data packet corruption occurring between 2 nodes in the communication link [24]. Several CRC implementation techniques have been described for various applications, ranging from the embedded [24] and wireless networks [25] to the communication protocols like the USB 3.0 [26]. Their popularity and acceptance is based on their encoding and decoding performance, simplicity, and reliable error detection [11]. With an increase in the data throughput, optimised CRC techniques must be implemented. Enhancing the CRC implementation from the software perspective involves the optimisation of the population of polynomials or determining ways to reduce the initial search for the set of polynomials within a population. Selecting differing polynomials for a particular word length or bit length is essential during optimisation.

The main objective while determining an appropriate CRC polynomial must ensure optimization, i.e., maximizing the Hamming Distance (HD) and minimizing the Hamming Weight (HW). Conventionally, these polynomials are determined by trying all the probable cases of the

polynomials along with their data bit errors (1, 2, and 3-bit message length errors), and thereafter, the most optimal polynomial is selected. Though this technique is suited for a smaller word length or polynomial degree, the larger data values show a high computational complexity and no solution can be generated.

In this paper, we have attempted to decrease the computational complexity using the Genetic Algorithm (GA), which treats the issue as an optimization problem. The GA is an evolutionary type of a computation method. However, no single definition can differentiate this technique from other evolutionary computation methods. Despite this fact, the GA method shows some common characteristic features, like the population of chromosomes, fitness-based selection, crossover for generating new offspring and a random mutation in the new offspring [27]. The GA helps in reducing the population size of the problem set by carrying out a directed search [28]. This feature is in direct contract with the conventional methods, which are of a random nature and involve the investigation of all the members present in the population of a problem set.

The data integrity of the transferred data packets is ensured with the help of data encryption. One principle to secure the operations of the cypher is diffusion. This can be satisfied when the single bit of plain text is altered, as each bit in the cypher text is seen to change at the 0.5 probability and vice versa. This can be very helpful for the current situation as any errors occurring in the messages during the data transmission could lead to numerous errors within the message which could be useful for the next step (i.e., CRC detector) to decrease the undetected error number. This number is further decreased by ensuring that every data packet consists of a header that is known by the sender and the receiver. Hence, if this error remains undetected by the Frame Check Sequence (FCS), it is further detected by determining any change made in the header after the decryption.

In this paper, we have used the Advanced Encryption Standard (AES) specification for all encryption-related functions for the headers. This specification [29] is defined as the block cypher that is used in 2 ways, i.e., for encrypting information within a cypher text and decrypting the resulting cypher text to its actual format. This is a symmetric-key algorithm, where the same key can be used for the encryption and the decryption functions. It encrypts data in 128-bit blocks by applying 128, 192, and 256-bit cryptographic keys. Here, we have used the 128-bit cryptographic keys.

For validating this proposed methodology, we carried out experiments in a MATLAB environment using the in-built GA toolbox. We used a 112-data word size, with a highest probable polynomial degree of 16. All bit error cases ranged between 1 and 6 bits, while a maximum of 400,000 combinations was investigated for every case. A minimum HD constraint value of 6 was used.

Table 1 presents the resulting polynomial, number of undetected errors, number of undetected errors with the encryption, and number of undetected errors with encryption with the header having a 1-byte size, and 4 million combinations of the 8-bit errors were randomly selected and tested. A data of 112-bit word size was used. The main advantage of including the encryption and the header is clearly observed. Without the encryption and the header, 141 undetected error probabilities are observed. However, the addition of the encryption decreased this number to 60, while the addition of header and encryption decreased this number further as shown in Table 1 the undetected error decrease from 141 to 0, thereafter, assisting the CRC technique to determine all the probable errors.

Table 1
Number of undetected error probabilities for the 0x8948 polynomial

Polynomial	CRC	CRC and Encryption	CRC and Encryption with Header
0x8948	141	60	0

C. Simulation Model

For evaluating the effect of an enhanced CRC polynomial on an AODV protocol, we compared the performance of the AODV protocol having a CRC polynomial and generated by the GA with a standard benchmark technique [30].

The model has been simulated in MATLAB environment. All experiments assumed a primary scenario comprising of a human who was waving his hands over his head, while the second scenario described a person carrying out a stand-up and sit-down action. For evaluating the human body movements, the authors used the dataset developed earlier in [31]. This dataset consisted of many general human activities. We attached 20 sensors (1-20) to a human body and these sensors communicated via Node 45 through the 24 relay nodes (21-44). The design is depicted in Figure 2.

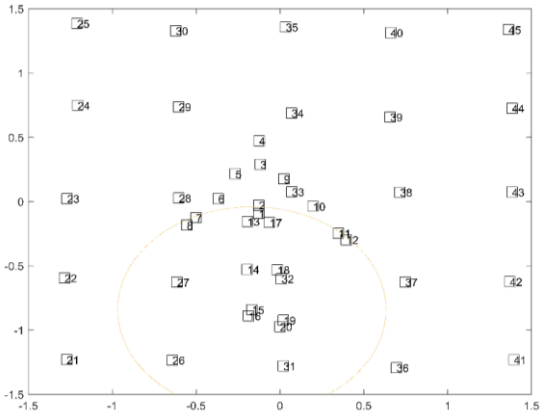

Figure 2: Location map of the sensor nodes

In both the cases (AODV [32] protocol with or without an enhanced CRC integration), we carried out experiments till we observed a notable difference. We have carried out 7 experiments, each lasting for 1500 sec. Some of the channels between the nodes were presumed as optimal, while others were presumed to follow the Gilbert-Elliott model. In Table 2, we described the nodes transmitted in the channels, modelled on the Gilbert-Elliot design, during these experiments.

It could be seen that every sensor-generated data packets which used 2 Poisson random variables. One of them determined the number of the data packets that were generated, while the other estimated the time interval between the generation of the data packets. They adopted a power consumption model described in [33]. Also, 2 activities from the dataset described by [34] were used for determining the trajectories of the body joints during the hand waving and the sit-down /stand-up experiments. All significant node parameters are described in Table 3, while Table 4 presents the Gilbert-Elliott channel parameters used. Table 5 represents the parameters of GA algorithm.

Table 2
Nodes transmitting in the GE-modelled channels

Experiment	Nodes
1	38
2	38 28
3	38 28 34
4	38 28 34 35
5	38 28 34 35 39
6	38 28 34 35 39 40
7	38 28 34 35 39 40 44

Table 3
Important node parameters

Parameter	Value
Coverage zone radius	0.8 m
Message length	112 bit
CRC polynomial	1 0 0 0 1 0 0 1 0 1 0 0 1 0 0 0 1
Data buffer size	100 packet
Data packet life time	10 second
Inter-arrival time	6 second
Mean of generation data packets	5 packet
Route request time out	2 second

Table 4
Gilbert-Elliott channel parameters

Parameter	Value
b Pr[Si=B | Si-1=G]	0.2
g Pr[Si=G | Si-1=B]	0.6
Error probability in bad state PB	0.1
Error probability in good state PG	0

Table 5
Genetic Algorithm parameters

Parameters	Values
Population size	45
Chromosome length	16
Maximum number of generation	60
Selection rate	0.8
Crossover rate	0.8
Mutation rate	0.2

IV. Results and Analysis

Figures 3 and 4 describe the PDR values for the hand-waving and the stand-up scenarios, respectively. Clearly, the AODV protocol with the improved CRC polynomial resulted in higher PDR values, as the corrupted data packets were resent.

Figures 5 and 6 describe the overhead for the two scenarios, respectively, for every experiment. Clearly, the AODV protocol with the improved CRC polynomial resulted in higher overhead values, as a novel control message was used. The increase was insignificant since it provided a better PDR, in return.

Figures 7 and 8 present the values for the E2E delay for the two scenarios. A lesser E2E delay was noted when the improved CRC protocol was used since many of the corrupted data packets were filtered and eliminated.

Figures 9 and 10 present the energy consumption values for the 2 scenarios. It could be noted that the use of an AODV protocol with the improved CRC polynomial resulted in higher energy consumption because the data packets were retransmitted and the error messages were sent [35].

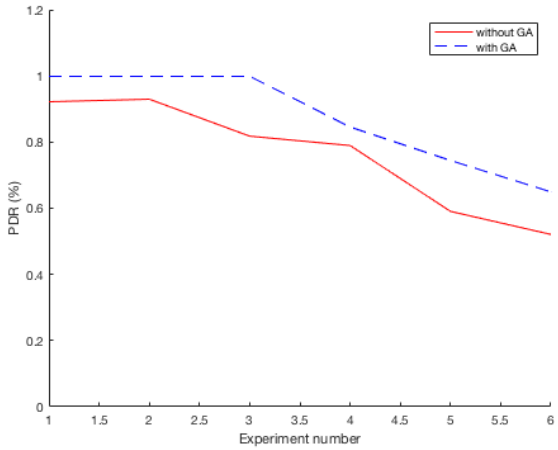

Figure 3: Performance evaluation of PDRs for the hand waving scenario with and without GA for 6 experiment attempts

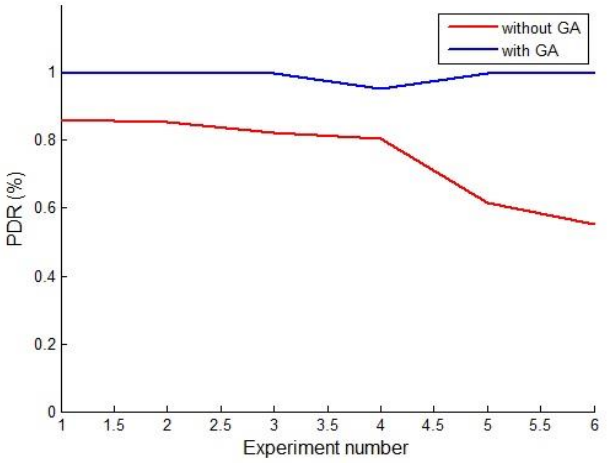

Figure 4: Performance evaluation of PDRs for the stand-up scenario with and without GA for 6 experiment attempts

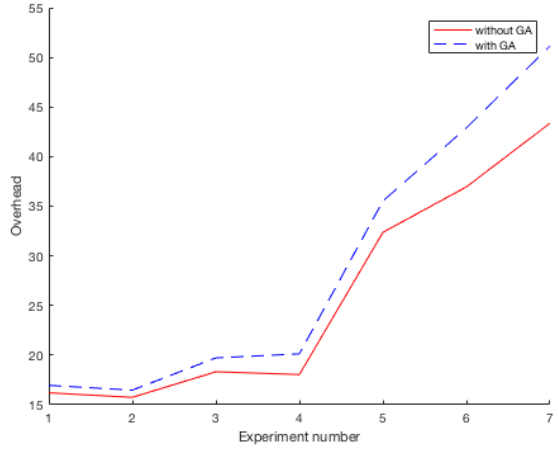

Figure 5: Performance evaluation of overhead for the hand waving scenario with and without GA for 7 experiment attempts

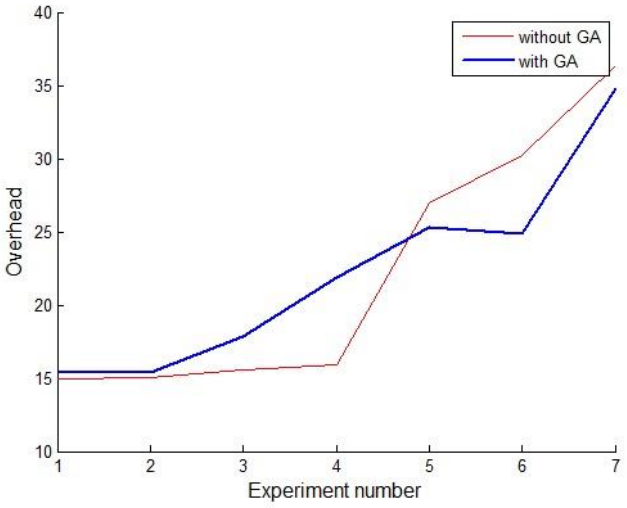

Figure 6: Performance evaluation of overhead for the stand-up scenario with and without GA for 7 experiment attempts

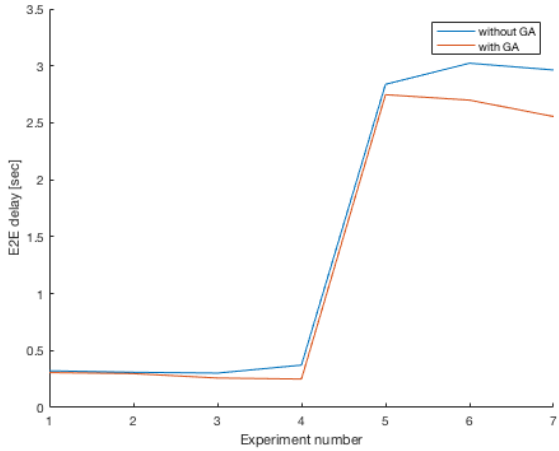

Figure 7: Performance evaluation of E2Es for the hand waving scenario with and without GA for 7 experiment attempts

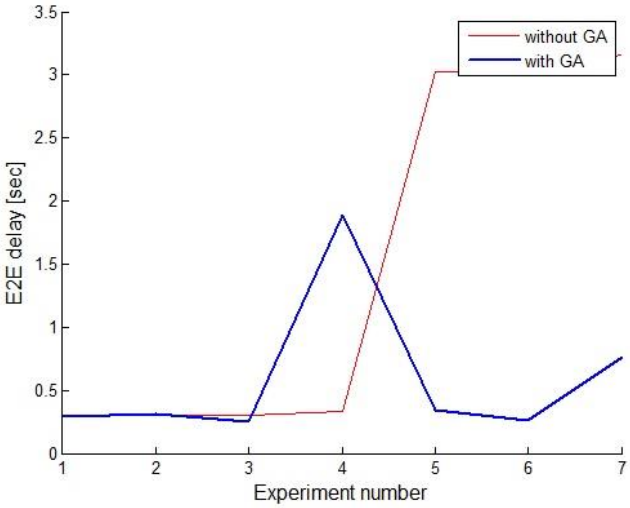

Figure 8: Performance evaluation of E2Es for the stand-up scenario with and without GA for 7 experiment attempts

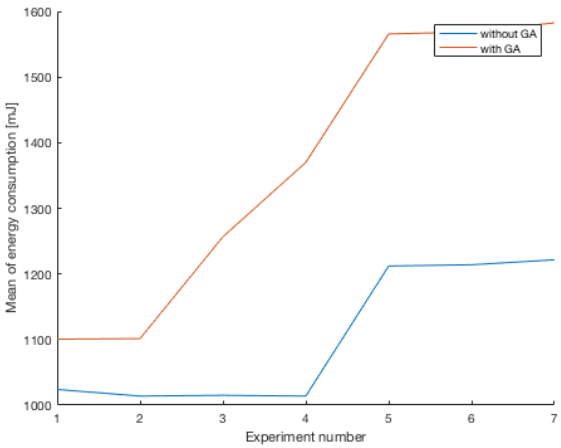

Figure 9: Performance evaluation of energy consumption for the hand waving scenario with and without GA for 7 experiment attempts

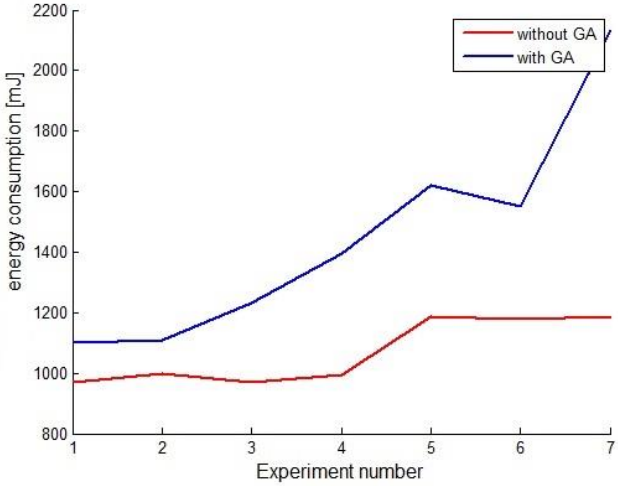

Figure 10: Performance evaluation of energy consumption for the stand-up scenario with and without GA for 7 experiment attempts

V. CONCLUSION

The high number of communication errors observed in the WBANs is concerning. The CRCs are helpful in maintaining the data transmission integrity and are seen to be influenced by the selected polynomial. In this paper, we developed and proposed a novel methodology for improving the CRC polynomials with the help of a heuristic search, and using the resulting CRCs and the encryption for enhancing the error detection in the WBANs.

The results have shown that this method was fairly successful since it led to an increase in the PDR and a decrease in the E2E delay. Also as expected, the overhead showed higher values because of the use of a novel control message type. The energy consumption also increased because of the error messages being sent and a retransmission of the data packets. This was not a serious problem as it could be presumed that this proposed technique was operational only during some particular scenarios, when the medium was subjected to noise or if the data was highly critical. The disadvantages of this technique were outweighed by the advantages due to data integrity and the performance of the proposed scheme.

REFERENCES

[1] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. E. Hadadi, "Attacks against aodv routing protocol in mobile ad-hoc networks," in 2016

13th international conference on computer graphics, imaging and visualization (cgiv), 2016, pp. 385–389.
[2] M. Quwaider and S. Biswas, "On-body packet routing algorithms for body sensor networks," in Networks and communications, 2009. netcom '09. first international conference on, 2009, pp. 171–177.
[3] N. Jamali and L. C. Fourati, "SKEP: A secret key exchange protocol using physiological signals in wireless body area networks," in Wireless networks and mobile communications (wincom), 2015 international conference on, 2015, pp. 1–7.
[4] Hassan, M. H., & Muniyandi, R. C. (2017). An Improved Hybrid Technique for Energy and Delay Routing in Mobile Ad-Hoc Networks. International Journal of Applied Engineering Research, 12(1), 134-139.
[5] Kumar, S. S., Manimegalai, P., & Karthik, S. (2018). A rough set calibration scheme for energy effective routing protocol in mobile ad hoc networks. Cluster Computing, 1-7.
[6] D. Sethi and P. P. Bhattacharya, "A study on energy efficient and reliable data transfer (eerdt) protocol for wban," in 2016 second international conference on computational intelligence communication technology (cict), 2016, pp. 254–258.
[7] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, vol. PP, no. 99, pp. 1–12, 2016.
[8] E. Abedini and A. Rezai, "A modified digital to digital encoding method to improve the wireless body area network (wban) transmission," in 2015 2nd international conference on knowledge-based engineering and innovation (kbei), 2015, pp. 1067–1070.
[9] B. Sansoda, S. Choomchuay, S. Timakul, and W. Khattiya, "Performance evaluation of ldpc codes on patterned wban data," in TENCON 2014 - 2014 ieee region 10 conference, 2014, pp. 1–4.
[10] AL-Dhief, F. T., Muniyandi, R. C., & Sabri, N. (2016). Performance Evaluation of LAR and OLSR Routing Protocols in Forest Fire Detection using Mobile Ad-Hoc Network. Indian Journal of Science and Technology, 9(48).
[11] T. Baicheva, S. Dodunekov, and P. Kazakov, "Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy," IEE Proceedings - Communications, vol. 147, no. 5, pp. 253–256, Oct. 2000.
[12] K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in 2008 4th international conference on wireless communications, networking and mobile computing, 2008, pp. 1–5.
[13] Z. Xu, Y. Jin, W. Shu, X. Liu, and J. Luo, "Sred: A secure reputation-based dynamic window scheme for disruption-tolerant networks," in MILCOM 2009-2009 ieee military communications conference, 2009, pp. 1–7.
[14] S. Sharma, "Energy-efficient secure routing in wireless sensor networks," PhD thesis, National Institute of Technology Rourkela, 2009.
[15] F. C. Lee, W. Goh, and C. K. Yeo, "A queuing mechanism to alleviate flooding attacks in probabilistic delay tolerant networks," in Telecommunications (aict), 2010 sixth advanced international conference on, 2010, pp. 329–334.
[16] S. Gupta, S. K. Dhurandher, I. Woungang, A. Kumar, and M. S. Obaidat, "Trust-based security protocol against blackhole attacks in opportunistic networks." in WiMob, 2013, pp. 724–729.
[17] S. Hyun, P. Ning, A. Liu, and W. Du, "Seluge: Secure and dos-resistant code dissemination in wireless sensor networks," in Proceedings of the 7th international conference on information processing in sensor networks, 2008, pp. 445–456.
[18] M. Jeyalakshmi, "Location aware end-end data security using mac for secured wireless sensor networks," in Advances in engineering, science and management (icaesm), 2012 international conference on, 2012, pp. 478–484.
[19] E. N. Gilbert, "Capacity of a burst-noise channel," The Bell System Technical Journal, vol. 39, no. 5, pp. 1253–1265, sept 1960.
[20] E. O. Elliott, "Estimates of error rates for codes on burst-noise channels," Bell system technical journal, vol. 42, no. 5, pp. 1977–1997, 1963.
[21] M. Mushkin and I. Bar-David, "Capacity and coding for the gilbert-elliott channels," IEEE Transactions on Information Theory, vol. 35, no. 6, pp. 1277–1290, Nov. 1989.
[22] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," 2003.
[23] Jubair, M., & Muniyandi, R. (2016). NS2 Simulator to Evaluate the Effective of Nodes Number and Simulation Time on the Reactive Routing Protocols in MANET. International Journal of Applied Engineering Research, 11(23), 11394-11399.
[24] P. Koopman and T. Chakravarty, "Cyclic redundancy code (crc) polynomial selection for embedded networks," in Dependable systems and networks, 2004 international conference on, 2004, pp. 145–154.
[25] V. Chea, M. V. Martin, and R. Liscano, "Hamming distance as a metric for the detection of crc-based side-channel communications in 802.11 wireless networks," in Communications and network security (cns), 2015 ieee conference on, 2015, pp. 218–226.
[26] Y. Wu and Y. Qiu, "The 8-bit parallel crc-32 research and implementation in usb 3.0," in Computer science service system (csss), 2012 international conference on, 2012, pp. 1079–1082.
[27] M. Mitchell, An introduction to genetic algorithms. Bradford Books, 1998.
[28] S. Sivanandam and S. Deepa, Introduction to genetic algorithms. Springer Berlin Heidelberg, 2007.
[29] "Specification for the advanced encryption standard (AES)." Federal Information Processing Standards Publication 197, 2001.
[30] Khirbeet, A. S., & Muniyandi, R. C. (2017). New Heuristic Model for Optimal CRC Polynomial, 7(1), 521–525. https://doi.org/10.11591/ijece.v7i1.pp521-525.
[31] Ding, W., Liu, K., Cheng, F., & Zhang, J. (2015). STFC: Spatio-temporal feature chain for skeleton-based human action recognition. Journal of Visual Communication and Image Representation, 26, 329–337. https://doi.org/10.1016/j.jvcir.2014.10.009.
[32] Das, D., Majumder, K., & Dasgupta, A. (2015). Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory. Procedia Computer Science, 54, 92–101. https://doi.org/10.1016/j.procs.2015.06.011.
[33] J. Toutouh, S. Nesmachnow, and E. Alba, "Fast energy-aware olsr routing in vanets by means of a parallel evolutionary algorithm," Cluster computing, vol. 16, no. 3, pp. 435–450, 2013.
[34] L. Xia, C. Chen, and J. Aggarwal, "View invariant human action recognition using histograms of 3D joints," in Computer vision and pattern recognition workshops (cvprw), 2012 ieee computer society conference on, 2012, pp. 20–27.
[35] Akkaya, K., & Younis, M. (2004). Energy-aware delay-constrained routing in wireless sensor networks. International Journal of Communication Systems, 17(6), 663-687.