LIGHTWEIGHT IDENTITY BASED ONLINE/OFFLINE SIGNATURE SCHEME FOR WIRELESS SENSOR NETWORKS

ANSER GHAZZAAL ALI ALQURAISHEE

UNIVERSITI TEKNOLOGI MALAYSIA

LIGHTWEIGHT IDENTITY BASED ONLINE/OFFLINE SIGNATURE SCHEME FOR WIRELESS SENSOR NETWORKS

ANSER GHAZZAAL ALI ALQURAISHEE

A thesis submitted in fulfilmentof the
requirements for the award of the degree of
Doctor of Philosphy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

MAY 2022

ACKNOWLEDGMENT

I contacted many individuals, researchers, academics, and practitioners during the preparation of this thesis. They have contributed to my thoughts and understanding. I particularly wish to express my sincere appreciation for my encouragement, guidance, criticism, and friendship to my main thesis supervisor, Professor Dr. Naomi Binti Salim. This thesis would not have been the same as presented here without her continued support and interest.

I am also indebted to Universiti Teknologi Malaysia (UTM) for providing my Ph. D research with an outstanding opportunity. UTM librarians and staff at the School of Computing are also particularly grateful for their help in supplying the relevant literature.

My sincere appreciation also extends to all of my peers and others who have helped on different occasions. Their views and tips are, indeed, helpful. Unfortunately, it is impossible in this limited space to list all of them. To all the members of my family, I am grateful.

ABSTRACT

Data security is one of the issues during data exchange between two sensor nodes in wireless sensor networks (WSN). While information flows across naturally exposed communication channels, cybercriminals may access sensitive information. Multiple traditional reliable encryption methods like RSA encryption-decryption and Diffie–Hellman key exchange face a crisis of computational resources due to limited storage, low computational ability, and insufficient power in lightweight WSNs. The complexity of these security mechanisms reduces the network lifespan, and an online/offline strategy is one way to overcome this problem. This study proposed an improved identity-based online/offline signature scheme using Elliptic Curve Cryptography (ECC) encryption. The lightweight calculations were conducted during the online phase, and in the offline phase, the encryption, point multiplication, and other heavy measures were pre-processed using powerful devices. The proposed scheme uniquely combined the Inverse Collusion Attack Algorithm (CAA) with lightweight ECC to generate secure identitybased signatures. The suggested scheme was analyzed for security and success probability under Random Oracle Model (ROM). The analysis concluded that the generated signatures were immune to even the worst Chosen Message Attack. The most important, resource-effective, and extensively used on-demand function was the verification of the signatures. The low-cost verification algorithm of the scheme saved a significant number of valued resources and increased the overall network's lifespan. The results for encryption/decryption time, computation difficulty, and key generation time for various data sizes showed the proposed solution was ideal for lightweight devices as it accelerated data transmission speed and consumed the least resources. The hybrid method obtained an average of 66.77% less time consumption and up to 12% lower computational cost than previous schemes like the dynamic IDB-ECC two-factor authentication key exchange protocol, lightweight IBE scheme (IDB-Lite), and Korean certification-based signature standard using the ECC. The proposed scheme had a smaller key size and signature size of 160 bits. Overall, the energy consumption was also reduced to 0.53 mJ for 1312 bits of offline storage. The hybrid framework of identity-based signatures, online/offline phases, ECC, CAA, and low-cost algorithms enhances overall performance by having less complexity, time, and memory consumption. Thus, the proposed hybrid scheme is ideally suited for a lightweight WSN.

ABSTRAK

Keselamatan data ialah salah satu isu semasa pertukaran data antara dua nod sensor dalam rangkaian sensor wayarles (WSN). Walaupun maklumat mengalir merentasi saluran komunikasi yang terdedah secara semula jadi, penjenayah siber boleh mencapai maklumat sensitif. Pelbagai kaedah penyulitan tradisional yang boleh dipercayai seperti penyulitanpenyahsulitan RSA dan pertukaran kunci Diffie-Hellman menghadapi krisis sumber perkomputeran disebabkan storan yang terhad, keupayaan perkomputeran yang rendah dan kuasa yang tidak mencukupi dalam WSN ringan. Kerumitan mekanisme keselamatan ini mengurangkan jangka hayat rangkaian, dan strategi dalam talian/luar talian adalah satu cara untuk mengatasi masalah ini. Kajian ini mencadangkan skim tandatangan dalam talian/luar talian berasaskan identiti yang lebih baik menggunakan penyulitan Kriptografi Lengkung Eliptik (ECC). Pengiraan ringan telah dijalankan semasa fasa dalam talian dan dalam fasa luar talian, penyulitan, pendaraban mata dan langkah berat lain telah dilaksanakan pra-pemprosesan menggunakan peranti berkuasa tinggi. Skim yang dicadangkan secara unik menggabungkan Algoritma Serangan Pakatan Songsang (CAA) dengan ECC ringan untuk menjana tandatangan berasaskan identiti yang selamat. Skim yang dicadangkan telah dianalisis untuk keselamatan dan kebarangkalian kejayaan di bawah Model Ramalan Rawak (ROM). Analisis menyimpulkan bahawa tandatangan yang dihasilkan adalah kebal walaupun terhadap Serangan Mesej Terpilih yang paling buruk. Fungsi atas permintaan yang paling penting, berkesan dari segi sumber dan digunakan secara meluas ialah pengesahan tandatangan. Algoritma pengesahan skim berkos rendah menjimatkan sejumlah besar sumber bernilai dan meningkatkan jangka hayat keseluruhan rangkaian. Keputusan dari segi masa penyulitan/penyahsulitan, kesukaran pengkomputeran dan masa penjanaan kunci untuk pelbagai saiz data menunjukkan penyelesaian yang dicadangkan adalah sesuai untuk peranti ringan kerana ia mempercepatkan kelajuan penghantaran data dan menggunakan sumber paling sedikit. Kaedah hibrid memperoleh purata 66.77% pengurangan penggunaan masa dan sehingga 12% kos pengiraan lebih rendah daripada skim sebelumnya seperti protokol pertukaran kunci pengesahan dua faktor dinamik IDB-ECC, skim IBE ringan (IDB-Lite) dan piawaian pensijilan tandatangan Korea yang berasaskan ECC. Skim yang dicadangkan mempunyai saiz kunci dan saiz tandatangan yang lebih kecil, iaitu 160 bit. Secara keseluruhan, penggunaan tenaga juga dikurangkan kepada 0.53 mJ untuk 1312bit storan luar talian. Rangka kerja hibrid bagi tandatangan berasaskan identiti, fasa dalam talian/luar talian, ECC, CAA dan algoritma kos rendah meningkatkan prestasi keseluruhan dengan mengurangkan kerumitan, masa dan penggunaan memori. Oleh itu, skim hibrid yang dicadangkan sangat sesuai untuk WSN yang ringan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AKA	-	Authenticated Key Agreement
BP	-	Bilinear Pairing
BS	-	Base Station
CA	-	Certificate Authority
CDHP	-	Computational Diffie-Hellman Problem
CFFS	-	Cluster-Based False Data Filtering Scheme
CH	-	Cluster Head
CL-PKC	-	Certificate less - Public Key Cryptography
CTAKA	-	Certificate less Key Agreement Two-Party Authenticated Key Agreement
DDHP	-	Decisional Diffie-Hellman Problem
DHP	-	Diffie-Hellman Problem
DHT	-	Distributed Hash Table
DLP	-	Discrete Logarithm Problem
DoS	-	Denial Of Service
DSEDA	-	Digital Signature Assisted End-To-End Data Authentication
ECC	-	Elliptic Curve Cryptography
ECC	-	Elliptic Curve Cryptography
ECDLP	-	Elliptic Curve Discrete Logarithm Problem
ECDSA	-	Elliptic Curve Digital Signature Algorithm
GDHP	-	Gap Diffie-Hellman Problem
GPS	-	Global Positioning System
HMAC	-	Keyed-Hashing for Message Authentication
IBC	-	Identity Based Cryptography
ID	-	Identity
ID	-	Identity
ID-2PAKA	-	Identity-Based Two-Party Authenticated Key Agreement
IHA	-	Interleaved Hop-By-Hop Authentication
KGC	-	Key Generation Centre
LBRS	-	Location-Based Resilient Secrecy

LEAP	-	Localized Encryption and Authentication Protocol
LEDS	-	Location-Aware End-To-End Data Security
LNCS	-	Location-Aware Network-Coding Security
LSSS	-	Linear Secret Sharing Scheme
MAC	-	Message Authentication Code
MAP	-	Message Authentication Polynomial
MKMP	-	Multi-BS Key Management Protocol
OOS	-	Online/Offline Signature
P2P	-	Peer-To-Peer
PK	-	Public Key
PKC	-	Public Key Cryptography
PKG	-	Private Key Generator
PKI	-	Public Key Infrastructure
SEF	-	Statistical En-Route Filtering
SHA	-	Secure Hash Algorithm
SK	-	Secret Key
WSN	-	Wireless Sensor Network

LIST OF SYMBOLS

k	-	Security Parameter
$param$	-	System Parameters
s	-	Master Secret Key of PKG / KGC
P_{pub}	-	Public Key of PKG / KGC
ID_i	-	The Identity of The User
$D_i = (s_i, R_i)$	-	Partial-Private-Key of User Identity ID_iGenerated by KGC In Cl-PKC
si	-	Secret Key in IBC or Secret-Value Chosen by KGC Of User IdentityID_i
R_i	-	Public Key in IBC or Public-Value Computed by KGC of User Identity ID_i
x_i	-	Secret-Value Chosen by User with Identity ID_i
P_i	-	Public-Key Computed by User with Identity ID_i
$sk_i = (s_i, x_i)$	-	Private Key of User Identity *Idi*
$pk_i = (R_i, P_i)$	-	Public Key of User Identity Id_i
m	-	Message
$U = ID_1, \cdots, ID_n$	-	Set of Parties with Each Party *Idi*
$A(A_I/A_{II})$	-	Adversary (Type I / Type Ii)
C	-	Challenger, Who Responds Adversary's Queries
L_i	-	List Maintained by Challenger
G, G_1, G_2, G_T	-	The Cyclic Group Composed of The Points On E/F_qOf Prime Order $q \geq 2k$
q, n	-	Prime Order of a Group
P	-	A Generator of Group G_1
$\hat{e}: G1 \times G1 \rightarrow G2$	-	Bilinear Pairing
H_0, H_1	-	Hash Functions
A	-	Alice
B	-	Bob
esk_A, t_A, epk_B, t_B	-	Ephemeral-Secret-Key of Alice and Bob Respectively

t_i, t_j	-	Ephemeral-Secret-Key of Party I with Intended Partner Party J
epk_A, T_A, epk_B, T_B	-	Ephemeral-Public-Key of Alice and Bob Respectively
T_i, T_j	-	Ephemeral-Public-Key of Party I with Intended Partner Party J
K_{AB}, K_{BA}	-	Secret Shared Key by Alice and Bob Respectively
sk	-	Secret Session Key
$\prod_{i,j}^{s}$	-	The sthSession Runs for Party $i$with Intended Partner Party j

CHAPTER 1

INTRODUCTION

1.1 Introduction

Wireless Sensor Network (WSN) consists of independent sensor devices having spatial distribution (Lee et al., 2004). These devices examine ecological and physical variations, e.g., smoke, level of pressure and temperature, humidity, etc. (Rashid and Rehmani, 2016). Information technologies like ubiquitous computing, edge computing, fog computing, and cloud computing are rapidly developing on-demand of sensor data computation. The user can avail conveniently the wireless communication techniques. The wireless network can offload data from the source node to the destination gateway without a costly wired connection. WSNs have been a broad focus area of research as an essential technique for business and academic circles. WSN has been installed commercially and industrially for numerous practical applications, like continuous field monitoring, military detecting, tracking, measuring traffic flow, environmental pollutant tracking, and many more (Gkikopouli et al., 2012, Ali et al., 2017, Bal, 2014, Zhang and Zhang, 2012).

High-performance, secured, and authenticated communication between two WSN nodes is essential. It is required to take care of the decision-making, message encryption, identification of the nodes, and smart consumption of resources (Bonetto et al., 2012). Sensor nodes generally have minimal resources in terms of battery, storage, transmission, and computing. The actual cost of an efficient and secure transmission between the two nodes is relatively high regarding energy usage (Das, 2009). Due to high energy constraints, WSNs are prone to various challenges for safety and furnishing authenticity than the traditional wired networks. However, there are various guidelines for low energy consumption in security provisions, such as smaller-sized authentication keys, lower computational and communication overheads, and algorithms where fewer keys are to be stored.

The Online/offline computing strategy is vital. It reduces the computing burden from sensor nodes hence increasing the lifespan of the network. The wireless sensor network is now needed to extend encryption to sensor-reliant operations in areas with different limitations that have not generally been subject to encryption. Lightweight cryptography is a technique that has been researched and developed to resolve this difficulty. The lightweight cryptography function allows the use of secure message encryption, even for devices with limited resources. One of the most significant security-related threats is cyber-attack by traditional IT systems to WSNs while using sensor devices for data collection from the real world. For example, a WSN has been deployed in a manufacturing plant for continuous monitoring and implementing independent control in a substantive environment. WSN gateways gather environmental data like temperature, humidity through a vast range of mounted sensors. The aim of utilizing sensors in the plant is to advance output and maintenance considerably. Incorrect analysis results would be induced if sensor data were falsified during this process, and erroneous control would result from such an occurrence that could potentially lead to significant damage. Moreover, since measurement data and control commands are trade secrets associated with production and management know-how, the prevention of leakage from a competitive point of view is also essential. Even if there is currently no problem, the effect of upcoming threats must be considered. Figure 1.1 shows that encryption can effectively respond to threats on WSNs, implying confidentiality and integrity data protection during message transfer between two WSN nodes.

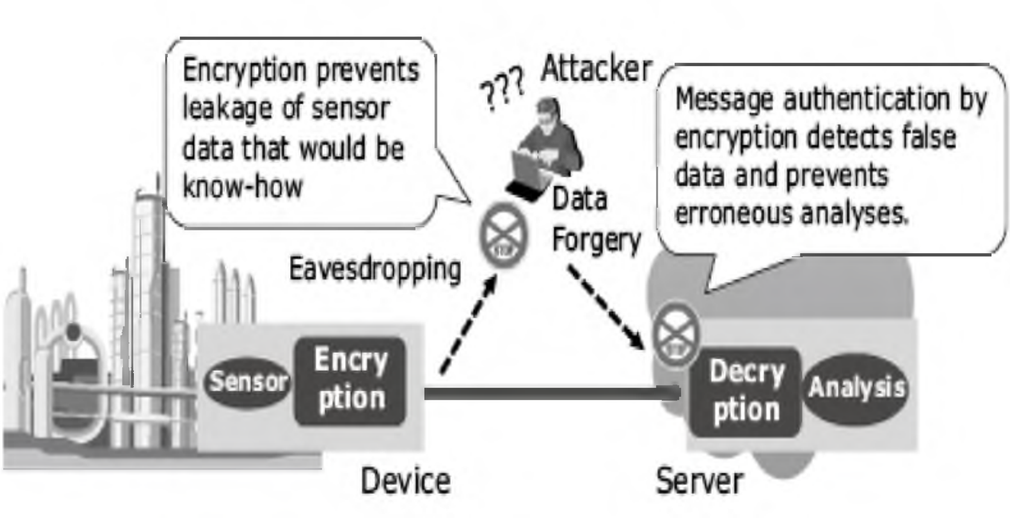

Figure 1-1 Encryption-based counter-measure against data collection threats

Encryption has already been applied as a standard on the communication system, in the data link layer, such as in a cell phone. In such a case, encryption in the application layer effectively provides end-to-end data protection from the device to the server. It ensures security independently of the communication system (Figure 1.2). Encryption should then be applied to the sensor devices, application processes, and additional resources and should be as light as possible. Lightweight cryptography could be a possible solution to ensure security during data transfer between two WSN nodes.

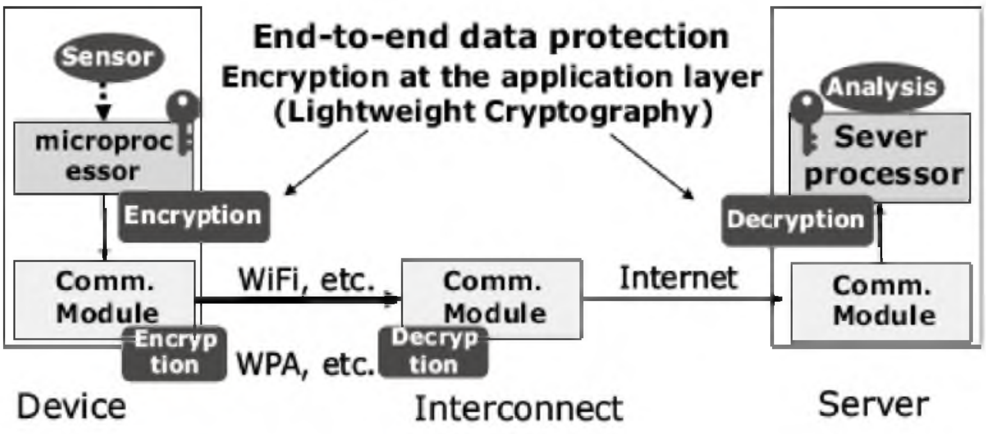

Figure 1-2 Example of lightweight cryptography applications

1.2 Problem Background

Wireless sensor networks are usually designed for hostile and unsupervised environments. These environments expose the sensors to numerous active and passive cyber intrusions (Burhanuddin et al., 2018; Cheikhrouhou, 2016). Sensor nodes are the key source of sensitive physical information in WSN. The low resources make them most vulnerable as they are unable to afford resource-hungry security schemes. The pairwise key exchange between a source and destination node utilizes a critical pre-distribution technique for intrusion prevention in a conventional network. However, most key-pairing cryptography follows complex algorithms and has high energy and storage consumption as RSA does in a wired network. Others focus on specific intrusion detection, regardless of overall communication performance.

Hence, research is required to discover a framework with resource consumption suitable for resource-constrained lightweight devices. The framework should consider all of these issues like efficient computation, smaller memory requirement, power-efficient and secures data exchange. Data integrity and information confidentiality can be achieved by incorporating a security mechanism that utilizes message authentication codes and packet encryption. Intrusion detection algorithms should control network access to endure WSN by legitimate nodes only. Authentication assures the network's entities that the packet originated from the sender from which it claims to originate. The network's reliability can only be established once the network has an efficient and secure shared key distribution system amongst the nodes inside the network. The appropriate level of security applications inside the WSN is a difficult task and requires overcoming several challenges. The problem background of WSN-related security stated these following issues:

- A low-cost, secure communication link between two individual nodes is one of the most challenging and crucial issues lightweight devices face in WSN.

- Most available signature schemes are unsuitable against existential forgery attacks for wireless sensor network systems due to several restrictions such as small storage space.

- The low battery life of the WSN nodes cannot afford the lengthy key generation procedure. Therefore, most existing security algorithms are not suitable for wireless sensor nodes.

- WSN nodes are highly bandwidth sensitive. Therefore, most of the online-based security procedures, demanding prolonged steps to be established, are not suitable for WSNs.

In this situation, secure and efficient cryptographic lightweight protocols like critical key establishment, mutual authentication, and identity-based signature schemes are necessitated to protect the information exchange between two neighboring communicated sensor nodes (Cohen et al., 2018; Tomić and McCann, 2017).

hybrid solution also helps to reduce algorithm complexity while imposing it on real-world challenges in terms of energy and memory consumption.

1.3.2 Constraints of Resources

Signature-based intrusion detection (ID) has four functional steps: data packet receiving, comparing with predefined database, identifying possible intrusion, and restricting the packet exchange mechanism (if an intrusion is detected). These cryptography algorithms operate using two key generations, namely private and public keys, between two neighboring nodes. Standard algorithms like RSA/DSA need a minimum 512 modulus and a maximum of 15360 sizes in bits key size in terms of computational effort for cryptoanalysis. Thus, the low-cost, secure communication link between two WSN nodes is one of the most challenging and crucial issues to use secure RSA/DSA, as the key size is comparatively large. In this situation, lightweight protocol identity-based signature schemes are suitable to protect the information exchange between two neighboring communicated sensor nodes. In contrast to RSA/DSA, lightweight Elliptic Curve Cryptography has a minimum 112-bit and maximum 512-bit key size. Therefore, the suitable algorithm selection for WSN nodes is highly challenging.

1.3.3 Standard Activities

The majority of WSN protocols are publicly known and do not consider potential security built in the stage of designing. Literature survey states that only a few numbers of security solutions are feasible to implement into real-time WSNs like identity-based online/offline key encryption, the Diffie Hellman key exchange algorithm, and elliptic curve cryptography. As the nodes of the WSNs are inconstant and have limitations in terms of battery capacity, memory capacity, it isn't easy to force security solutions into already built WSNs. Therefore, the solution must be incorporated while designing the WSN. The solution must be compatible with the wireless protocols and sensor behaviors.

deceives. This thesis followed to find out a solution for this particular problem statement:

"How to implement a compatible and efficient signcryption scheme based on an improved elliptic curve digital signature algorithm through online/offline methods suitable for lightweight wireless sensor devices?"

1.5 Research Objectives

This research aims to develop the optimal identity-based signcryption security based on ECDSA with an Online/Offline approach for providing security to digital signatures in WSNs environment, to improve the complexity, cost, time, and energy consumption. Thus, support fast and efficient communication. This study mainly focuses on implementing a signcryption scheme for communication security in WSNs. The following three objectives are established to achieve the goal of this research:

I. **To develop an improved identity-based, online/offline signature scheme, using key encryption with elliptic curve pairing and Diffie-Hellman problem for lightweight WSN**: The existing cryptography-based algorithms are primarily complex and consume a lot of resources. Online/offline signature design, elliptic curve, and Diffie-Hellman solutions are used in several security schemes. A competent combination of such solutions could help to provide security to lightweight WSN exceptionally. An improved identity-based, online/offline signature scheme using key encryption with elliptic curve pairing and Diffie-Hellman problem is expected to be helpful in this situation. The solution is also expected to reduce algorithm complexity, save energy, cost of memory, time for lightweight WSNs.

II. **To develop security analysis of the proposed algorithms using Random Oracle Model**: Random Oracle Model (ROM) is a scheme based on the Cryptographic Hash Function (CHF) (Khalili et al., 2020). Hashing is an

The third phase presents the research implementation, testing, and performance evaluation of this research's proposed techniques.

Chapter 4 details the proposed signcryption security framework based on the identity-based online/offline signature schemes and random oracle model. The results and discussion of the proposed techniques and comparing the results with other existing schemes are also presented and discussed.

Chapter 5 presents the conclusion, describes the contributions made by this study, and suggests future directions. This chapter also introduces the set objectives and comparative performance evaluations' achievements.

REFERENCES

ADEEL, A., GOGATE, M., FAROOQ, S., IERACITANO, C., DASHTIPOUR, K., LARIJANI, H. & HUSSAIN, A. 2019. A survey on the role of wireless sensor networks and IoT in disaster management. *Geological disaster monitoring based on sensor networks.* Springer.

AHLAWAT, P. AND DAVE, M., 2018. An attack model-based highly secure key management scheme for wireless sensor networks. *Procedia Computer Science*, *125*, pp.201-207.

ALCHIHABI, A., DERVIS, A., EVER, E. & AL-TURJMAN, F. 2019. A generic framework for optimizing performance metrics by tuning parameters of clustering protocols in WSNs. *Wireless Networks,* 25**,** 1031-1046.

ALGHAMDI, T. A. 2019. Convolutional technique for enhancing security in wireless sensor networks against malicious nodes. *Human-centric Computing and Information Sciences,* 9**,** 38.

ALI, A., MING, Y., CHAKRABORTY, S. & IRAM, S. 2017. A comprehensive survey on real-time applications of WSN. *Future internet,* 9**,** 77.

AMISH, P. & VAGHELA, V. 2016. Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. *Procedia computer science,* 79**,** 700-707.

AMJAD, M., SHARIF, M., AFZAL, M.K. AND KIM, S.W., 2016. TinyOS-new trends, comparative views, and supported sensing applications: A review. *IEEE Sensors Journal*, *16*(9), pp.2865-2889.

AZARMEHR, M., AHMADI, A. & RASHIDZADEH, R. Secure authentication and access mechanism for IoT wireless sensors. 2017 IEEE International Symposium on Circuits and Systems (ISCAS), 2017. IEEE, 1-4.

BAL, M. Industrial applications of collaborative wireless sensor networks: A survey. 2014 IEEE 23rd international symposium on industrial electronics (ISIE), 2014. IEEE, 1463-1468.

BALA, S., SHARMA, G. & VERMA, A. K. 2016. PF-ID-2PAKA: pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks. *Wireless Personal Communications,* 87**,** 995-1012.

BALAKRISHNAN, S., IVY, B. P. U. & ILANGO, S. S. 2018. A Novel And Secured Intrusion Detection System For Wireless Sensor Networks Using Identity Based Online/Offline Signature. *ARPN Journal of Engineering and Applied Sciences,* 13**,** 8544-8547.

BASHIRPOUR, H., BASHIRPOUR, S., SHAMSHIRBAND, S. & CHRONOPOULOS, A. T. 2018. An improved digital signature protocol to multi-user broadcast authentication based on elliptic curve cryptography in wireless sensor networks (WSNs). *Mathematical and Computational Applications,* 23**,** 17.

BELLARE, M. & ROGAWAY, P. Random oracles are practical: A paradigm for designing efficient protocols. Proceedings of the 1st ACM conference on Computer and communications security, 1993. 62-73.

BHANDARI, S., BERGMANN, N., JURDAK, R. & KUSY, B. 2017. Time-series data analysis of wireless sensor network measurements of temperature. *Sensors,* 17**,** 1221.

BLAKE-WILSON, S., JOHNSON, D. & MENEZES, A. Key agreement protocols and their security analysis. IMA international conference on cryptography and coding, 1997. Springer, 30-45.

BONEH, D. & FRANKLIN, M. 2003. Identity-based encryption from the Weil pairing. *SIAM journal on computing,* 32**,** 586-615.

BONETTO, R., BUI, N., LAKKUNDI, V., OLIVEREAU, A., SERBANATI, A. & ROSSI, M. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. 2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM), 2012. IEEE, 1-7.

BOUAZIZ, M. & RACHEDI, A. 2016. A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. *Computer Communications,* 74**,** 3-15.

BRAEKEN, A. 2020. Symmetric Key-Based Authentication with an Application to Wireless Sensor Networks. *IoT Security: Advances in Authentication***,** 65-84.

BURHANUDDIN, M., MOHAMMED, A. A.-J., ISMAIL, R., HAMEED, M. E., KAREEM, A. N. & BASIRON, H. 2018. A review on security challenges and features in wireless sensor networks: IoT perspective. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* 10**,** 17-21.

CANETTI, R. & KRAWCZYK, H. Analysis of key-exchange protocols and their use for building secure channels. *International Conference on the Theory and Applications of Cryptographic Techniques,* 2001. Springer, 453-474.

CHALLA, S., WAZID, M., DAS, A.K., KUMAR, N., REDDY, A.G., YOON, E.J. AND YOO, K.Y., 2017. *Secure signature-based authenticated key establishment scheme for future IoT applications. Ieee Access*, 5, pp.3028-3043.

CHANTI, Y., NAIK, D. K. S., MOTHE, R., YAMSANI, N. & BALIJA, S. 2018. A modified Elliptic Curve Cryptography Technique for Securing Wireless Sensor Networks. *International Journal Of Engineering &Technology*.

CHEIKHROUHOU, O. 2016. Secure group communication in wireless sensor networks: a survey. *Journal of Network and Computer Applications,* 61, 115-132.

CHEN, J., TANG, S., HE, D. & TAN, Y. 2017. Online/offline signature based on UOV in wireless sensor networks. *Wireless Networks,* 23, 1719-1730.

CHENG, Z., NISTAZAKIS, M., COMLEY, R. AND VASIU, L., 2005. On The Indistinguishability-Based Security Model of Key Agreement Protocols-Simple Cases. *IACR Cryptol. ePrint Arch., 2005*, p.129.

CHOI, H.-W. & KIM, H. 2017. Cryptanalysis on Efficient Two-factor User Authentication Scheme with Unlinkability for Wireless Sensor Networks. *International Journal of Applied Engineering Research,* 12, 3933-3937.

COHEN, A., COHEN, A. & GUREWITZ, O. Secured Data Gathering Protocol for IoT Networks. International Symposium on Cyber Security Cryptography and Machine Learning, 2018. Springer, 129-143.

CUI, J., ZHANG, Y., CAI, Z., LIU, A. AND LI, Y., 2018. Securing display path for security-sensitive applications on mobile devices. *Computers, Materials and Continua*, *55*(1), p.17.

DAHSHAN, M. H. 2017. Robust data authentication for unattended wireless sensor networks. *Telecommunication Systems,* 66, 181-196.

DAS, A. K., SHARMA, P., CHATTERJEE, S. & SING, J. K. 2012. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications,* 35, 1646-1656.

DAS, M. L. 2009. Two-factor user authentication in wireless sensor networks. *IEEE transactions on wireless communications,* 8, 1086-1090.

DENER, M. & BAY, O. F. 2017. Practical Implementation of an Adaptive Detection-Defense Unit against Link Layer DoS Attacks for Wireless Sensor Networks. *Security and Communication Networks,* 2017.

DIFFIE, W. & HELLMAN, M. 1976. New directions in cryptography. *IEEE transactions on Information Theory,* 22**,** 644-654.

DU, H., WEN, Q. & ZHANG, S. 2019. An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network. *IEEE Access,* 7**,** 42683-42693.

DUAN, Y., LI, W., FU, X., LUO, Y. & YANG, L. 2017. A methodology for reliability of WSN based on software defined network in adaptive industrial environment. *IEEE/CAA Journal of Automatica Sinica,* 5**,** 74-82.

DUCHE, R. N. & SARWADE, N. P. 2013. Sensor node failure detection based on round trip delay and paths in WSNs. *IEEE Sensors journal,* 14**,** 455-464.

ELHOSENY, M., YUAN, X., EL-MINIR, H. K. & RIAD, A. M. 2016. An energy efficient encryption method for secure dynamic WSN. *Security and Communication Networks,* 9**,** 2024-2031.

EVEN, S., GOLDREICH, O. AND MICALI, S., 1989, August. On-line/off-line digital signatures. In *Conference on the Theory and Application of Cryptology* (pp. 263-275). Springer, New York, NY.

FAN, X. & GONG, G. 2012. Accelerating signature-based broadcast authentication for wireless sensor networks. *Ad Hoc Networks,* 10**,** 723-736.

FERNG, H.-W. & KHOA, N. M. 2017. On security of wireless sensor networks: a data authentication protocol using digital signature. *Wireless Networks,* 23**,** 1113-1131.

GAN, X., WANG, Z., SHEN, L., LIU, C. & LAI, X. 2011. Parallelizing cryptographic hash function using relaxed encryption framework. *Chinese journal of electronics,* 20.

GAO, Y., ZENG, P., CHOO, K.-K. R. & SONG, F. 2016. An Improved Online/Offline Identity-Based Signature Scheme for WSNs. *IJ Network Security,* 18**,** 1143-1151.

GKIKOPOULI, A., NIKOLAKOPOULOS, G. & MANESIS, S. A survey on underwater wireless sensor networks and applications. 2012 20th Mediterranean conference on control & automation (MED), 2012. IEEE, 1147-1154.

GRUMĂZESCU, C. & PATRICIU, V.-V. 2018. A Comprehensive Survey on ID-Based Cryptography for Wireless Sensor Networks. *Journal of Military Technology Vol,* 1.

GUAN, Y. & GE, X. 2017. Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks. *IEEE Access,* 5**,** 10858-10870.

GUO, F., MU, Y. & CHEN, Z. Identity-based online/offline encryption. International Conference on Financial Cryptography and Data Security, 2008. Springer, 247-261.

GUPTA, K. & SILAKARI, S. 2011. Ecc over rsa for asymmetric encryption: A review. *International Journal of Computer Science Issues (IJCSI),* 8**,** 370.

GURA, N., PATEL, A., WANDER, A., EBERLE, H. & SHANTZ, S. C. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. International workshop on cryptographic hardware and embedded systems, 2004. Springer, 119-132.

HADY, R. & AGRANOVSKY, A. Crypto miracles with random oracle. IEEE-Siberian Workshop of Students and Young Researches. Modern Communication Technologies SIBCOM-2001. Proceedings (Cat. No. 01EX452), 2001. IEEE, 20-22.

HALIM, T. & ISLAM, M. R. 2012. A study on the security issues in WSN. *International Journal of Computer Applications,* 53.

HANKERSON, D., MENEZES, A. J. & VANSTONE, S. 2006. *Guide to elliptic curve cryptography,* Springer Science & Business Media.

HANKERSON, D., VANSTONE, S. & MENEZES, A. 2004. Cryptographic protocols. *Guide to Elliptic Curve Cryptography***,** 153-204.

HARIA, P. B. & SINGHB, S. N. 2019. Security Analysis Framework in Wireless Sensor Networks.

HARN, L. & REN, J. 2011. Generalized digital certificate for user authentication and key establishment for secure communications. *IEEE Transactions on Wireless Communications,* 10**,** 2372-2379.

HUNG, C.W. AND HSU, W.T., 2018. Power consumption and calculation requirement analysis of AES for WSN IoT. *Sensors*, *18*(6), p.1675.

IQBAL, U. & SHAFI, S. 2019. A provable and secure key exchange protocol based on the elliptical curve diffe–hellman for wsn. *Advances in big data and cloud computing.* Springer.

JADHAV, R. & VATSALA, V. 2017. Security issues and solutions in wireless sensor networks. *International Journal of Computer Applications,* 162**,** 14-19.

JALADI, A. R., KHITHANI, K., PAWAR, P., MALVI, K. & SAHOO, G. 2017. Environmental monitoring using wireless sensor networks (WSN) based on IOT. *Int. Res. J. Eng. Technol,* 4**,** 1371-1378.

JOYE, M. & QUISQUATER, J.-J. 2004. *Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004, Proceedings*, Springer.

KANNHAVONG, B., NAKAYAMA, H., NEMOTO, Y., KATO, N. & JAMALIPOUR, A. 2007. A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless communications,* 14**,** 85-91.

KAR, J. 2014. Provably Secure Online/Off-line Identity-Based Signature Scheme for Wireless Sensor Network. *IJ Network Security,* 16**,** 29-39.

KARGARAN, E., MANSTRETTA, D. & CASTELLO, R. 2017. Design and Analysis of 2.4 GHz $30~\mu\text {W} $ CMOS LNAs for Wearable WSN Applications. *IEEE Transactions on Circuits and Systems I: Regular Papers,* 65**,** 891-903.

KARLOF, C., SASTRY, N. & WAGNER, D. TinySec: a link layer security architecture for wireless sensor networks. Proceedings of the 2nd international conference on Embedded networked sensor systems, 2004. 162-175.

KARTHIKEYAN, S., PATAN, R. AND BALAMURUGAN, B., 2019. Enhancement of security in the Internet of Things (IoT) by using X. 509 authentication mechanism. In *Recent Trends in Communication, Computing, and Electronics* (pp. 217-225). Springer, Singapore.

KAUR, P. & GURM, J. 2016. Detect and prevent HELLO FLOOD attack using centralized technique in WSN. *Int. J. Comput. Sci. Eng. Technol,* 7**,** 379-381.

KAUSHAL, K. & SAHNI, V. 2015. DoS attacks on different layers of WSN: A review. *International Journal of Computer Applications,* 130.

KHALILI, M., DAKHILALIAN, M. & SUSILO, W. 2020. Efficient chameleon hash functions in the enhanced collision resistant model. *Information Sciences,* 510**,** 155-164.

KOBLITZ, N. 1987. Elliptic curve cryptosystems. *Mathematics of computation,* 48**,** 203-209.

KOBLITZ, N. & MENEZES, A. J. 2015. The random oracle model: a twenty-year retrospective. *Designs, Codes and Cryptography,* 77**,** 587-610.

KUDLA, C. & PATERSON, K. G. Modular security proofs for key agreement protocols. International conference on the theory and application of cryptology and information security, 2005. Springer, 549-565.

KULAU, U., ROTTMANN, S., SCHILDT, S., VAN BALEN, J. & WOLF, L. Undervolting in real world wsn applications: A long-term study. 2016 International Conference on Distributed Computing in Sensor Systems (DCOSS), 2016. IEEE, 9-16.

KUMAR, M. & GUPTA, P. 2019. An efficient and authentication signcryption scheme based on elliptic curves. *MATEMATIKA: Malaysian Journal of Industrial and Applied Mathematics,* 35**,** 1-11.

KUMAR, R., TRIPATHI, S. & AGRAWAL, R. 2020. An Analysis and Comparison of Security Protocols on Wireless Sensor Networks (WSN). *Design Frameworks for Wireless Networks.* Springer.

KUMAR, V., JAIN, A. & BARWAL, P. 2014. Wireless sensor networks: security issues, challenges and solutions. *International Journal of Information and Computation Technology (IJICT),* 4**,** 859-868.

LAI, J., MU, Y. & GUO, F. 2017. Efficient identity-based online/offline encryption and signcryption with short ciphertext. *International Journal of Information Security,* 16**,** 299-311.

LAI, J., MU, Y., GUO, F. & SUSILO, W. Improved identity-based online/offline encryption. Australasian Conference on Information Security and Privacy, 2015. Springer, 160-173.

LAMACCHIA, B., LAUTER, K. & MITYAGIN, A. Stronger security of authenticated key exchange. International conference on provable security, 2007. Springer, 1-16.

LEE, J.-J., KRISHNAMACHARI, B. & KUO, C.-C. Impact of heterogeneous deployment on lifetime sensing coverage in sensor networks. 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004., 2004. IEEE, 367-376.

LI, F., ZHONG, D. & TAKAGI, T. 2012. Practical identity-based signature for wireless sensor networks. *IEEE Wireless Communications Letters,* 1**,** 637-640.

LI, M., CHEN, L., ZHAO, J., ZHANG, Q. & LIU, Y. 2008. Signature-file-based approach for query answering over wireless sensor networks. *IEEE transactions on vehicular technology,* 57, 3146-3154.

LING, C.-H., LEE, C.-C., YANG, C. C. & HWANG, M.-S. 2017. A Secure and Efficient One-time Password Authentication Scheme for WSN. *IJ Network Security,* 19, 177-181.

LIPARE, A., EDLA, D.R. AND KUPPILI, V., 2019. Energy efficient load balancing approach for avoiding energy hole problem in WSN using grey wolf optimizer with novel fitness function. *Applied Soft Computing*, *84*, p.105706.

LIPPOLD, G., BOYD, C. & NIETO, J. G. Strongly secure certificateless key agreement. International Conference on Pairing-Based Cryptography, 2009. Springer, 206-230.

LIU, A. & NING, P. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. 2008 International Conference on Information Processing in Sensor Networks (ipsn 2008), 2008. IEEE, 245-256.

LIU, B., YAN, Z. & CHEN, C. W. 2013a. MAC protocol in wireless body area networks for E-health: Challenges and a context-aware design. *IEEE Wireless Communications,* 20, 64-72.

LIU, J., ZHANG, Z., CHEN, X. & KWAK, K. S. 2013b. Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Transactions on parallel and distributed systems,* 25, 332-342.

LIU, J. K., BAEK, J., ZHOU, J., YANG, Y. & WONG, J. W. 2010. Efficient online/offline identity-based signature for wireless sensor network. *International Journal of Information Security,* 9, 287-296.

LIU, J. K. & ZHOU, J. An efficient identity-based online/offline encryption scheme. International Conference on Applied Cryptography and Network Security, 2009. Springer, 156-167.

LIU, X., YU, J., LI, F., LV, W., WANG, Y. & CHENG, X. 2019. Data aggregation in wireless sensor networks: from the perspective of security. *IEEE Internet of Things Journal.*

LU, X., YIN, W., WEN, Q., JIN, Z. & LI, W. 2018. A lattice-based unordered aggregate signature scheme based on the intersection method. *IEEE Access,* 6, 33986-33994.

LV, B., PENG, Z. & TANG, S. 2018. Precomputation Methods for UOV Signature on Energy-Harvesting Sensors. *IEEE Access,* 6, 56924-56933.

MAGONS, K. Applications and Benefits of Elliptic Curve Cryptography. SOFSEM (Student Research Forum Papers/Posters), 2016. 32-42.

MAHIMA, V., KANAGACHIDAMBARESAN, G., BALAJI, M. & DAS, J. 2019. Reliability Study of Sensor Node Monitoring Unattended Environment. *Smart Innovations in Communication and Computational Sciences.* Springer.

MALAN, D. J., WELSH, M. & SMITH, M. D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004., 2004. IEEE, 71-80.

MALLICK, C. & SATPATHY, S. 2018. Challenges and Design Goals of Wireless Sensor Networks: A State-of-the-art Review. *International Journal of Computer Applications,* 179, 42-47.

MARTÍNEZ, V. G., ENCINAS, L. H. & ÁVILA, C. S. 2011. Java Card implementation of the Elliptic Curve Integrated Encryption Scheme using prime and binary finite fields. *Computational Intelligence in Security for Information Systems.* Springer.

MATHUR, A., NEWE, T. & RAO, M. 2016. Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. *Sensors,* 16, 118.

MENEZES, A. J., OKAMOTO, T. & VANSTONE, S. A. 1993. Reducing elliptic curve logarithms to logarithms in a finite field. *iEEE Transactions on information Theory,* 39, 1639-1646.

MESHRAM, C., LEE, C.-C., MESHRAM, S. G. & MESHRAM, A. 2020. OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network. *IEEE Access,* 8, 80063-80073.

MESHRAM, C., POWAR, P. L., OBAIDAT, M. S., LEE, C.-C. & MESHRAM, S. G. 2018. Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs. *IET Networks,* 7, 363-367.

MIHAJLOVIĆ, Ž., MILOSAVLJEVIĆ, V., JOŽA, A. AND DAMNJANOVIĆ, M., 2017, May. Modular WSN node for environmental monitoring with energy harvesting support. In *2017 Zooming Innovation in Consumer Electronics International Conference (ZINC)* (pp. 41-44). IEEE.

MILLER, V. S. Use of elliptic curves in cryptography. Conference on the theory and application of cryptographic techniques, 1985. Springer, 417-426.

MITTAL, V., GUPTA, S. AND CHOUDHURY, T., 2018. Comparative analysis of authentication and access control protocols against malicious attacks in wireless sensor networks. In *Smart computing and informatics* (pp. 255-262). Springer, Singapore.

MODIEGINYANE, K. M., LETSWAMOTSE, B. B., MALEKIAN, R. & ABU-MAHFOUZ, A. M. 2018. Software defined wireless sensor networks application opportunities for efficient network management: A survey. *Computers & Electrical Engineering,* 66**,** 274-287.

MOHAMMADI, S., ATANI, R. E. & JADIDOLESLAMY, H. 2011. A comparison of routing attacks on wireless sensor networks. *organization,* 4**,** 21.

MOHAMMADI, S. & JADIDOLESLAMY, H. 2011. A comparison of physical attacks on wireless sensor networks. *International Journal of Peer to Peer Networks,* 2**,** 24-42.

MUGHAL, M.A., LUO, X., ULLAH, A., ULLAH, S. AND MAHMOOD, Z., 2018. A lightweight digital signature based security scheme for human-centered Internet of Things. *IEEE Access*, *6*, pp.31630-31643.

NG, H., SIM, M. & TAN, C. 2006. Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal,* 24**,** 138-144.

NIKUMBH, H. & SHAH, V. Hardware Implementation of Modular Multiplication. 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2018. IEEE, 376-380.

NIU, Q. 2014. ECDH-based Scalable Distributed Key Management Scheme for Secure Group Communication. *JCP,* 9**,** 153-160.

OULD AMARA, S., BEGHDAD, R. & OUSSALAH, M. 2013. Securing wireless sensor networks: A survey. *EDPACS,* 47**,** 6-29.

PAN, J.-S., DAO, T.-K., PAN, T.-S., NGUYEN, T., CHU, S. & RODDICK, J. 2017. An improvement of flower pollination algorithm for node localization optimization in WSN. *Journal of Information Hiding and Multimedia Signal Processing,* 8**,** 486-499.

POMANTE, L., PUGLIESE, M., MARCHESANI, S. & SANTUCCI, F. WINSOME: A middleware platform for the provision of secure monitoring services over Wireless Sensor Networks. 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013. IEEE, 706-711.

PRABHU, B., PRADEEP, M. & GAJENDRAN, E. 2016. Military applications of wireless sensor network system. *Military Applications of Wireless Sensor Network System (January 25, 2017). A Multidisciplinary Journal of Scientific Research & Education,* 2**,** 12.

PRAKASH, S. & RAJPUT, A. 2018. Hybrid cryptography for secure data communication in wireless sensor networks. *Ambient Communications and Computer Systems.* Springer.

QUINTERO, V.L., ESTEVEZ, C., ORCHARD, M.E. AND PÉREZ, A., 2018. Improvements of energy-efficient techniques in WSNs: a MAC-protocol approach. *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1188-1208.

RAJAN, A. A., SWAMINATHAN, A. & PAJILA, B. A Comparative Analysis of LEACH, TEEN, SEP and DEEC in Hierarchical Clustering Algorithm for WSN Sensors. Intelligent Communication Technologies and Virtual Mobile Networks, 2019. Springer, 395-403.

RAMSON, S. J. & MONI, D. J. Applications of wireless sensor networks—A survey. 2017 international conference on innovations in electrical, electronics, instrumentation and media technology (ICEEIMT), 2017. IEEE, 325-329.

RANI, A. & KUMAR, S. A survey of security in wireless sensor networks. 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), 2017. IEEE, 1-5.

RANI, S., AHMED, S. H., TALWAR, R. & MALHOTRA, J. 2017. Can sensors collect big data? An energy-efficient big data gathering algorithm for a WSN. *IEEE Transactions on Industrial Informatics,* 13**,** 1961-1968.

RASHID, B. & REHMANI, M. H. 2016. Applications of wireless sensor networks for urban areas: A survey. *Journal of network and computer applications,* 60**,** 192-219.

RATHOD, V. & MEHTA, M. 2011. Security in wireless sensor network: a survey. *Ganpat university journal of engineering & technology,* 1**,** 35-44.

REN, J., ZHANG, Y., ZHANG, K. & SHEN, X. 2016. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Transactions on Wireless Communications,* 15, 3718-3731.

REN, Y., LIU, Y., JI, S., SANGAIAH, A. K. & WANG, J. 2018. Incentive mechanism of data storage based on blockchain for wireless sensor networks. *Mobile Information Systems,* 2018.

SAKAI, R. & KASAHARA, M. 2003. ID based Cryptosystems with Pairing on Elliptic Curve. *IACR Cryptol. ePrint Arch.,* 2003, 54.

SANTOS-GONZÁLEZ, I., RIVERO-GARCÍA, A., BURMESTER, M., MUNILLA, J. & CABALLERO-GIL, P. 2020. Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. *Information Systems,* 88, 101423.

SARKAR, A., & SINGH, B. K. (2021). A multi-instance cancelable fingerprint biometric based secure session key agreement protocol employing elliptic curve cryptography and a double hash function. Multimedia Tools and Applications, 80(1), 799-829.

SAQIB, N. & IQBAL, U. Security in wireless sensor networks using ECC. 2016 IEEE International Conference on Advances in Computer Applications (ICACA), 2016. IEEE, 270-274.

SENTHILKUMAR, U. & SENTHILKUMARAN, U. 2016. Review of asymmetric key cryptography in wireless sensor networks. *International Journal of Engineering and Technology,* 8, 859-862.

SGORA, A., VERGADOS, D. D. & CHATZIMISIOS, P. 2016. A survey on security and privacy issues in wireless mesh networks. *Security and Communication Networks,* 9, 1877-1889.

SHAHZAD, F., PASHA, M. & AHMAD, A. 2017. A survey of active attacks on wireless sensor networks and their countermeasures. *arXiv preprint arXiv:1702.07136.*

SHAMIR, A. Identity-based cryptosystems and signature schemes. Workshop on the theory and application of cryptographic techniques, 1984. Springer, 47-53.

SHARMA, N. & BHATT, R. 2018. Privacy preservation in WSN for healthcare application. *Procedia computer science,* 132, 1243-1252.

SHARMA, U. & BAHL, N. 2017. A Review on Security Issues and Attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science,* 8.

SHEN, L., MA, J., LIU, X. & MIAO, M. 2016. A provably secure aggregate signature scheme for healthcare wireless sensor networks. *Journal of medical systems,* 40**,** 244.

SHIM, K.-A. 2017. BASIS: a practical multi-user broadcast authentication scheme in wireless sensor networks. *IEEE Transactions on Information Forensics and Security,* 12**,** 1545-1554.

SHIM, K.-A. & PARK, C.-M. 2014. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE transactions on parallel and distributed systems,* 26**,** 2128-2139.

SINGH, J., KUMAR, V. & KUMAR, R. 2016. An Efficient and Secure RSA Based Certificateless Signature Scheme for Wireless Sensor Networks. *Advances in Signal Processing and Intelligent Recognition Systems.* Springer.

SOGANI, A. & JAIN, A. 2019. Energy aware and fast authentication scheme using identity based encryption in wireless sensor networks. *Cluster Computing,* 22**,** 10637-10648.

SURYADEVARA, N., MUKHOPADHYAY, S., RAYUDU, R. & HUANG, Y.-M. Sensor data fusion to determine wellness of an elderly in intelligent home monitoring environment. 2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings, 2012. IEEE, 947-952.

SUSEELA, G. & PHAMILA, Y. A. V. 2018. Energy efficient image coding techniques for low power sensor nodes: A review. *Ain Shams Engineering Journal,* 9**,** 2961-2972.

SWANSON, C. & JAO, D. A study of two-party certificateless authenticated key-agreement protocols. International Conference on Cryptology in India, 2009. Springer, 57-71.

TAN, S.-Y. 2019. Correction to "Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing". *IEEE Access,* 7**,** 17045-17049.

TEYMOURZADEH, M., VAHED, R., ALIBEYGI, S. & DASTANPOUR, N. 2020. Security in wireless sensor networks: Issues and challenges. *arXiv preprint arXiv:2007.05111*.

THUMBUR, G., RAO, G.S., REDDY, P.V., GAYATHRI, N.B., REDDY, D.K. AND PADMAVATHAMMA, M., 2020. Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Internet of Things Journal*, *8*(3), pp.1908-1920.

TING, P.-Y., TSAI, J.-L. & WU, T.-S. 2017. Signcryption method suitable for low-power IoT devices in a wireless sensor network. *IEEE Systems Journal,* 12**,** 2385-2394.

TOMIĆ, I. & MCCANN, J. A. 2017. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal,* 4**,** 1910-1923.

UMA, M. & PADMAVATHI, G. 2013. A Survey on Various Cyber Attacks and their Classification. *IJ Network Security,* 15**,** 390-396.

VARGHESE, B., JOHN, N. E., SREELAL, S. & GOPAL, K. 2016. Design and development of an RF energy harvesting wireless sensor node (EH-WSN) for aerospace applications. *Procedia Computer Science,* 93**,** 230-237.

VERMA, G. K., SINGH, B. & SINGH, H. 2018. Provably secure message recovery proxy signature scheme for wireless sensor networks in e-healthcare. *Wireless Personal Communications,* 99**,** 539-554.

VINODHA, D. & ANITA, E. M. 2019. Secure data aggregation techniques for wireless sensor networks: a review. *Archives of Computational Methods in Engineering,* 26**,** 1007-1027.

WAN, H., MCCALLEY, J.D. AND VITTAL, V., 2000. Risk based voltage security assessment. *IEEE Transactions on Power Systems*, *15*(4), pp.1247-1254.

WANG, D., JIANG, Y., SONG, H., HE, F., GU, M. & SUN, J. 2017. Verification of implementations of cryptographic hash functions. *IEEE Access,* 5**,** 7816-7825.

WANG, D., BAI, B., ZHAO, W. AND HAN, Z., 2018. A survey of optimization approaches for wireless physical layer security. *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1878-1911.

WANG, D. AND TENG, J., 2018. Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc network. *电子与信息学报*, *40*(1), pp.11-17.

WANG, F., XU, G. & XU, G. 2019. A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map. *IEEE Access,* 7, 101596-101608.

WANG, J. & WANG, C. 2018. Full secure identity-based encryption scheme over lattices for wireless sensor networks in the standard model. *International Journal of High Performance Computing and Networking,* 12, 111-117.

WANG, Z. & CHEN, W. 2013. An ID-based online/offline signature scheme without random oracles for wireless sensor networks. *Personal and ubiquitous computing,* 17, 837-841.

WATERS, B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. Annual International Cryptology Conference, 2009. Springer, 619-636.

WU, S., NIU, J., CHOU, W. AND GUIZANI, M., 2016. Delay-aware energy optimization for flooding in duty-cycled wireless sensor networks. *IEEE Transactions on Wireless Communications*, *15*(12), pp.8449-8462.

XIAO, J.-F. & ZENG, G.-H. 2009. An improved ring signature scheme without trusted key generation center for wireless sensor network. *Journal of Shanghai Jiaotong University (Science),* 14, 189-194.

XIE, K., NING, X., WANG, X., HE, S., NING, Z., LIU, X., WEN, J. & QIN, Z. 2017. An efficient privacy-preserving compressive data gathering scheme in WSNs. *Information Sciences,* 390, 82-94.

XIE, Y., LI, X., ZHANG, S. & LI, Y. 2019. $ ICLAS $: An improved certificateless aggregate signature scheme for healthcare wireless sensor networks. *IEEE Access,* 7, 15170-15182.

XIAODONG, Y., FAYING, A., PING, Y., LIKUN, X., YUTONG, L., TINGCHUN, M. AND CAIFEN, W., 2018, March. A message authentication scheme for VANETs based on trapdoor hash function. In *2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA)* (pp. 279-282). IEEE.

XU, G. & XU, G. An ID-based blind signature from bilinear pairing with unlinkability. 2013 3rd International Conference on Consumer Electronics, Communications and Networks, 2013. IEEE, 101-104.

XU, J., WU, X. & XIE, X. Efficient Identity-Based Offline/Online Encryption Scheme for Lightweight Devices. 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 2018. IEEE, 569-575.

YANG, S.-K., SHIUE, Y.-M., SU, Z.-Y., LIU, I.-H. & LIU, C.-G. 2020. An authentication information exchange scheme in WSN for IoT applications. *IEEE Access,* 8, 9728-9738.

YAO, A. C.-C. & ZHAO, Y. 2012. Online/offline signatures for low-power devices. *IEEE Transactions on Information Forensics and Security,* 8, 283-294.

YOON, E.J. AND YOO, K.Y., 2005, July. More efficient and secure remote user authentication scheme using smart cards. In *11th International Conference on Parallel and Distributed Systems (ICPADS'05)* (Vol. 2, pp. 73-77). IEEE.

YUSSOFF, Y. M., HASHIM, H., ROSLI, R. & BABA, M. D. 2012. A review of physical attacks and trusted platforms in wireless sensor networks. *Procedia Engineering,* 41, 580-587.

ZAHOOR, S. & MIR, R. N. 2018. Resource management in pervasive Internet of Things: A survey. *Journal of King Saud University-Computer and Information Sciences*.

ZHANG, J., YU, W. & LIU, X. CRTBA: Chinese remainder theorem-based broadcast authentication in wireless sensor networks. 2009 International Symposium on Computer Network and Multimedia Technology, 2009. IEEE, 1-4.

ZHANG, S. & ZHANG, H. A review of wireless sensor networks and its applications. 2012 IEEE international conference on automation and logistics, 2012. IEEE, 386-389.

ZHANG, W., HAN, Y. & LIU, L. A novel key agreement protocol based on bilinear pairing. 2010 3rd International Conference on Biomedical Engineering and Informatics, 2010. IEEE, 2717-2720.

ZHANG, X., FU, X., HONG, L., LIU, Y. AND WANG, L., 2020. Provable secure identity-based online/offline encryption scheme with continual leakage resilience for wireless sensor network. *International Journal of Distributed Sensor Networks*, *16*(6), p.1550147720928733.

ZHANG, X., MA, S., HAN, D. & SHI, W. Implementation of elliptic curve Diffie-Hellman key agreement scheme on IRIS nodes. Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things, 2015. IEEE, 160-163.

ZHANG, Y. & ZHOU, W. An ECDSA signature scheme designs for PBOC 2.0 specifications. 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 2012. IEEE, 2106-2110.

ZHENG, Y. Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption). Annual international cryptology conference, 1997. Springer, 165-179.

ZHU, B., ADDADA, V. G. K., SETIA, S., JAJODIA, S. & ROY, S. Efficient distributed detection of node replication attacks in sensor networks. Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), 2007. IEEE, 257-267.

ZHU, J., ZOU, Y. & ZHENG, B. 2017. Physical-layer security and reliability challenges for industrial wireless sensor networks. *IEEE access,* 5**,** 5313-5320.

ZHU, W. T., ZHOU, J., DENG, R. H. & BAO, F. 2012. Detecting node replication attacks in wireless sensor networks: a survey. *Journal of Network and Computer Applications,* 35**,** 1022-1034.

ZOU, Y. & WANG, G. 2015. Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. *IEEE Transactions on Industrial Informatics,* 12**,** 780-787.