An Efficient Secure Protocol for Wireless Sensor Networks Based on Hybrid Approach

Irshad Ullah, Noor ul Amin, Jawaid Iqbal, Muhammad Shahid and Farman Ali

Department of Information Technology
Hazara University Mansehra
K-P, Pakistan

Abstract
Wireless Sensor Networks (WSNs) comprise of independent sensor nodes attached to one or more base stations. Conversely, the applied placement of sensor systems face various challenges enforced by everyday life demands. Wireless sensor nodes have restricted communication resources. Therefore, it is extremely unfavorable to use hard information security techniques. The aim of this paper is to develop an optimal and secure hybrid algorithm to provide secure data transfer and also increase the lifetime of the wireless sensor networks. In symmetric cryptographic algorithms the secure key distribution was a main problem, while asymmetric cryptographic algorithms is more costly for resource constrain environment of WSNs. To resolve these above issues, we encode and decode the messages through Advance Encryption Standard algorithm and securely exchange key using Hyper Elliptic Curve Cryptography (HECC) algorithm. This hybrid cryptographic scheme deeds the benefits of the symmetric and asymmetric cryptographic algorithms and is more secure and suitable for resource constrain environment of WSNs.

Keywords:
Security, Advance Encryption Standard (AES), Wireless Sensor Network (WSN), Hyper Elliptic Curve Cryptography (HECC), Communication and computational cost.

1. Introduction

Wireless Sensor Networks (WSN) is composed of fixed or moveable sensor nodes, which form the wireless network using self-organization and multi-hop method. Tts purpose is to cooperate finding, processing and communicating the object observing information in the network coverage areas. Sensor networks establish the three components sensor node, sink node and user node [1]. Wireless sensor networks have an unlimited susceptibility due to the transmission nature and risky environment. Wireless sensor networks suffer from various limitations such as short battery life, low processing capability and lesser memory[2]. Wireless sensor networks have been generally deployed in physical world for many applications such as conservational monitoring. Frequently, the conservational in which WSNs is worked is exposed to many security attacks [3]. Currently, network security is a significant feature in networking applications. Every day, billions of users exchange and generate useful information in several regions, such as legal, engineering, medical, banking and other fields through internetwork. The information must be secure against the unauthorized users, which is to be transferred [4].

Through certification mechanisms data communication systems can be avoided from illegal transfer and alteration. Message confirmation and identification needs to be observed. Consequently, the receiver has to confirm messages transmitted from the sensor node through WSNs. This work is done through cryptography. This is a challenge to find out appropriate cryptography for wireless sensor networks which could be computationally optimal, optimal in power and good storage capacity [5]. Cryptography is a science of transforming a clear message into unclear one, and then retransforming that message back to its original form. The cryptography can be used to authenticate the message between sender and receiver during wireless communication. There are two methods of cryptography, secret key cryptography also called symmetric key cryptography and public key cryptography also called asymmetric key cryptography [4].

There are a number of research challenges in wireless sensor networks. The use of Wireless Sensor Networks (WSNs) [6] [7] have considerably improved in different areas like health monitoring, environmental monitoring, biological and health care. The main challenges [8] in wireless sensor network include Real world protocol, query processing, programming abstractions, topology control, access control, data integrity, data confidentiality, data authentication, localization and dependability of nodes.

Two-phase hybrid cryptography algorithm [2] and Hybrid Cryptography for secure and optimal data Communication for WSNs [9] were proposed. The main joint problems of these schemes are security, high complexity and more communication overhead.

In this paper, we propose efficient secure protocol for WSNs based on hybrid approach, whose security and complexity trust will be based on the hardness of HECDLP (Hyper Elliptic Curve Discrete Logarithm Problem). NIST recommend symmetric 2^{80} bits key, RSA is 2^{1024} bits key, ECC is 2^{160} bits key and HECC is 2^{80} bits key. Proposed

Manuscript received June 5, 2018
Manuscript revised June 20, 2018

scheme use 2^{80} bit key to save the computation and communication cost and also increased the security level.
The key objective of this paper is to provide an optimal and secure data communication between sensor nodes and reduce the whole energy consumption of the WSNs. During data communication among sensor nodes, this scheme will provide an authentication, confidentiality and data integrity. In this paper, we improve the efficiency and security for wireless sensor network. The propose protocol is more secure and optimal from existing protocols.

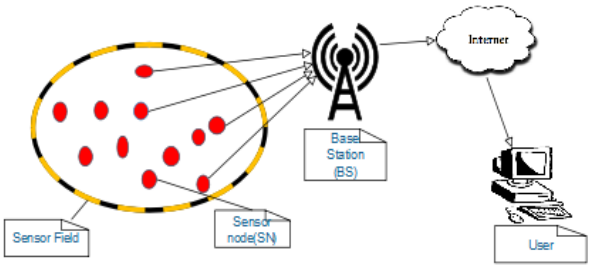

Fig. 1. General Architecture for Wireless Sensor Networks (WSNs)

A. Groundworks
Let suppose prime number p, here $p \geq 2^{80}$ and $\mathbf{F_p}$ is a finite field of order p. HCC $HC(Fp)$ over finite field $\mathbf{F_p}$ be define the Eq (a)

$$C: y2+h(x)y = f(x) \bmod p \quad (a)$$

Where $h(x) \in F[x]$ is a polynomial and degree $h(x) \leq g$ and $f(x) \in F[x]$ is a monic polynomial and degree of the $f(x) \leq 2g+1$ distinct points on EC, points on HEC do not form a group. Divisor is a finite prescribed sum of points on HEC and denoted in Mum-Ford form as

$$D = \big(u(x), v(x)\big) = \Big(\sum_{j=0}^{g} ujx^j, \sum_{j=0}^{g-1} vjx^j\Big)$$

The Divisor Jacobian Group $\mathbf{J_c}(\mathbf{F_p})$ and the order of Jacobian Group $\mathbf{o}\left(\mathbf{J_c}(\mathbf{F_p})\right)$is well defined as:

$$|(\sqrt{p}-1)^{2g}| \leq O\left(J_c(F_p)\right) \leq |(\sqrt{p}+1)^{2g}|$$

B. Types of Genus Curve
Genus curve g choose the time processing of the HECC such as encryption, decryption and generation of key.
Genus g=2

$$y2 = x5 + a_3x3 + a_2x2 + a_1x + a_0$$
Genus g=3 (b)

$$y2 = x7 + a_5x5 + a_4x4 + a_3x3 + a_2x2 + a_1x + a_0$$
Genus g= 4 (c)

$$y2 = x9 + a_7x7 + a_6x6 + a_5x5 + a_4x4 + a_3x3 + a_2x2 + a_1x + a_0$$
Genus g=5 (d)

$$y2 = x11 + a_9x9 + a_8x8 + a_7x7 + a_6x6 + a_5x5 + a_4x4 + a_3x3 + a_2x2 + a_1x + a_0$$
Genus g=6 (e)

$$y2 = x11 + a_9x9 + a_8x8 + a_7x7 + a_6x6 + a_5x5 + a_4x4 + a_3x3 + a_2x2 + a_1x + a_0$$ (f)

C. Description: Hyper Elliptic curve DLP
Let suppose D is the divisor of order n in the Jacobian group $\mathbf{J_c}(\mathbf{F_p})$ find an integer w $\in (\mathbf{F_p})$.
Such that:

$$D1 = w.D$$

The rest of the paper we organized the paper as follows. In the section 2 we discuss the literature review. In section 3 propose scheme have been discussed. In section 4 we discuss the analysis of security. In section 5 we discusses the analysis of performance. In last section 6 we write-down the conclusion of the propose paper.

2. Literature Review

The author [10] [11] propose an optimal security protocol for WSNs where both text and images data are encrypted through genetic operation and chaotic map. But this is a solid hardware based cryptosystem. Lightweight block ciphers and predictable block codes are three categories of encryption algorithm in WSNs. Solid hardware based cryptosystems due to high energy consumption and memory usage is not suitable for WSNs. Conventional block ciphers implemented in WSN but they are susceptible to many security attacks. To overcome these problem currently researcher focus on lightweight block ciphers.
In this paper [12] authors propose a novel scheme for communication authentication with hash-based approach, namely 2ArrayMD-160 (2AMD-160). The execution time and security achieved by the 2AMD-160 method are more effective than the SHA1 and MD5 methods. Here [13]

describe some types of attacks in wireless sensor network like Denial-of-Service Attack, Replicating a Node Attack, Routing Attack and Attacks on Information during transmission. Also describe security protocol (SPINS, Tiny Sec, Mini Sec, LEAP, Mini Sec and ZigBee) for WSNs to overcome these security problem and finally comparison among these security protocols.

Authors [14] analyzes the Advance Encryption algorithm (AES) for security purpose in WSNs. Public key cryptography has a less effectiveness and high energy consumption, in contrast to symmetric cryptography. AES consume very less time for encryption. When [15] increase the number of sensor nodes where symmetric based cryptographic scheme do not scale well. To eliminate these problems introduced public key base cryptographic approach is introduced. Here we discuss two efficient public key algorithm, Elliptic Curve Cryptography (ECC) and RSA (Rives, Shamir and Aleman) which are mostly use in wireless sensor networks. ECC found is more beneficial compare to RSA due to shorter key size, low memory usage and less CPU consumption. When cipher size and power consumption are the factors of consideration, the ECC (160 bits) is better than RSA (1024 bits).

The author [16] compared the three encryption algorithm, DES, AES and RSA based on encryption and decryption time. RSA algorithm takes more time to encryption or decryption process compared to the time taken by AES and DES algorithm. The evaluation from the simulation result, AES algorithm is much better than RSA and DES algorithm. DES [17] is breakable and vulnerable to some attacks. Symmetric key algorithms [5] uses single key to secure message among two users and entire networks. If network size is n then each users required n-1 keys. Public key cryptography removes the key distribution problem. It provides secured data communication among nodes and also condense the total energy consumption of the WSNs and also increases the network lifetime. Compare RSA with ElGamal algorithm, RSA increases the network lifetime and less computational power. RSA uses to provide for continuous monitoring in WSNs. ElGamal algorithm consumes 15% more energy than RSA algorithm and RSA algorithm provides better security for WSNs.

A Hybrid algorithm [18] was proposed. Here, DES algorithm is used for data communication because of its greater efficiency in block encryption, and RSA algorithm is used for the key encryption of the DES because of its managing benefits in key cipher. During the process of transferring encrypted data, 64-bit DES session key used by the random number generator only once. It encodes the original text to produce the cipher text. Instead, the sender acquires public key from public key managing center, and then RSA uses to encrypted session key. In last, send out the combination of the cipher text from Data Encryption Standard (DES) and encryption session key from RSA. This procedure is considered weak as using DES and RSA affects the security level.

The authors [19] proposed a solution for confident data communication in Wireless sensor networks in which they are using AES for data encryption/decryption and RSA algorithm is used for key generation, the main drawback in their work is that key size in RSA is very huge due to which it was extraordinary consuming of resources.

In [2] this paper authors have proposed a strong hybrid security algorithm for WSNs, and the result of this proposed algorithms illustration better security for reduced encryption/decryption time. The proposed solution complexity was very high. The author [9] proposed hybrid protocol for wireless sensor networks, which AES used for encryption/decryption and ECC for key exchanging. It provides high security level [20] appreciations to the enhancement in key size. They are checked authentication and confidentiality. Conversely, it is not suitable for the small size sensor nodes.

The authors [21] proposed HECC based efficient and secure authentication scheme, which are complex when data are increased. Encryption and decryption of using ECC and HECC technique are not suitable for large data [22]. ECC and HECC only uses for faster key generation. ECC 2^{160} bits key, HECC 2^{80} bits key (genus 2) and 2^{54} bits key (genus 3) are provided same security level [23] but genus 2 is best curve for hyper elliptic cryptosystem compared with other genus.

3. Proposed Scheme

In this scheme, we have proposed an optimal and secure scheme for Wireless Sensor Networks, they are an efficient and more secure from existing scheme. This scheme provides secure data communication for Wireless Sensor Networks. We have dig to solve the drawbacks exposed in the proposed previous works for the optimal and secure transmission in wireless sensor network. Advance encryption standard is the most effective private key algorithm for encoding and decoding of information that requires single key. AES operation with static key length i.e. 128,192 or 256 bits. The complexity of Hyper Elliptic Curve Cryptography (HECC) is directly-proportional to the transmitted data length. HECC an optimal and more secure than AES but HECC slower and high resources consuming due to asymmetric nature. In our proposed scheme we are using AES for the data encryption/decryption and HECC for the purpose of key generation and sharing. Here we prefer to HECC by ECC because HECC provided same security level with the use of much smaller key than ECC. Hence, HECC is faster and efficient than ECC for key exchange.

Table 1: Notation guide

Notation	Description
HC	Hyper Elliptic Curve
D	Divisor of the prime order $n \geq 2^{80}$
$hash$	One way hashed function
h_i / h_i'	hash values
BS	Base Station
R_n	Random number
S_i	Sensor node
IDsi	Identification ID for sensor
U_{node}	User node
Pu_{Unode}	Public key of user node
Pr_{Unode}	Private key of user node
Pr_{Si}	Private key of sensor node
Pu_{Si}	Public key of sensor node
C_i	Cipher text
Sk_i	Session key
XS_{Ki}	Encrypted session key
R_{ski}	Round Session Key
$\perp$	Rejection

There are four (4) stages of our proposed scheme:

- Setup Phase
- Session Key Generation and Node Authentication phase
- Secure Data Communication phase
- Key Update Phase

A. Setup Phase

In this phase, network administrator initially loads the public and private keys on user node. The public key of user node along with public key and private key of the wireless sensor node are loaded to sensor node and further all the public keys of wireless sensor nodes are loaded on user node (server).

B. Session Key Generation and Node Authentication phase

The main problem happening in symmetric algorithms was sharing of keys as the same keys were also used for both encryption/decryption of data. When key is released, then the privacy and security of the whole data to be transferred will be compromises.

To solve this problem, we are using public key algorithms, i.e. HECC for sharing keys

Algorithm 1.1

1. Wireless Sensor Node(Pu_{Si} , Pr_{Si} ,Pu_{Unode} , IDsi)
2. Generate $R_n \in_R \{0,1,2- - - -n\}$
3. h_i = hash(R_n || IDsi ||$Authentication$ IDi)
4. C_i = EPu_{Unode} (R_n || IDsi ||$Authentication$ IDi || h_i)
5. Transmit cipher text C_i to user node through BS
6. User node Decrypt (Pu_{Unode} , Pr_{Unode} , Pr_{Si})
7. R_n || IDsi ||$Authentication$ IDi || h_i) =**D**Pr_{Si} (C_i)
8. Calculated h_i' = hash (R_n || IDsi ||$Authentication$ IDi)
9. Accepted if $h_i' = h_i$
10. Otherwise $\perp$
11. Wireless Node Authentication(IDsi , $Authentication$ IDi)
12. Compare received Authentication IDi with stored $Authentication$ IDi
13. If match correct
14. Than Node legal
15. else Node illegal and Blacklisted
16. Session key generation and encryption/decryption (R_{n1} , $R_{n\,2}$ …. R_{nn})
17. S_i , $S_j \in$ (R_{n1} , $R_{n\,2}$ …. R_{nn})
18. Calculate session key by using randomly selection of the two random numbers $S_{Ki} = R_{ni} \oplus R_{nj}$
19. Using HECC XS_{Ki} = **E**Pu_{Unode} (S_{Ki})
20. Encrypted session key (XS_{Ki}) send encrypted session key to user nodes
21. S_{Ki} = **D**Pr_{Unode} (S_{Ki})
22. Session key = S_{Ki}

C.Secure Data Communication phase

In our proposed scheme we used Advance Encryption standard (AES) which are fast and most effective algorithm for data encryption and decryption. We will be using AES 192 bits key for data encryption/decryption.

Following steps are involved in data encryption and decryption

- Firstly, data will be divided into two blocks of 128 bits.
- The size of keys will be 192 bit.
- On this data 12th rounds of AES will be performed.
- The encrypted data will be sent through the public network to the receiver node.
- For decryption, receiver will be used AES to get the real data and HECC will be used for secure key exchange.

The following two algorithm 1.2 algorithm for encryption and 1.3 algorithm for decryption.

Encryption Algorithm 1.2

For each wireless sensor node $S_i \in$ area/environment

1. Sense critical data of environment D_{ri}
2. Calculate hash value h_i = hash(D_{ri})
3. Calculate C_{ri} = E_{Rski} (D_{ri} , h_i)
4. Disseminate C_{ri} to user node through Base Station(BS)

End

Decryption Algorithm 1.3

For each wireless sensor node encipher data $C_{ri} \in$ area/environment.

1. (D_{ri} , h_i = D_{Rski} (C_{ri})
2. Calculate h_i' = hash(D_{ri})

3. Accept if Calculate $h_i' = h_i$ some data of particular area otherwise $\perp$

End

D. Key Update Phase

In this phase key will be change after specific interval of time. It will be provide backward secrecy and forward secrecy.

Algorithm 1.4

1. User node calculated round session key R_{ski}
2. Randomly select two random numbers e.g. R_{ni} and R_{nj}
3. Than calculate session key $R_{ski} = R_{ni}\ XOR\ R_{nj}$
4. Now for next coming session this session key (R_{ski}) will be used which provide forward secrecy and backward secrecy

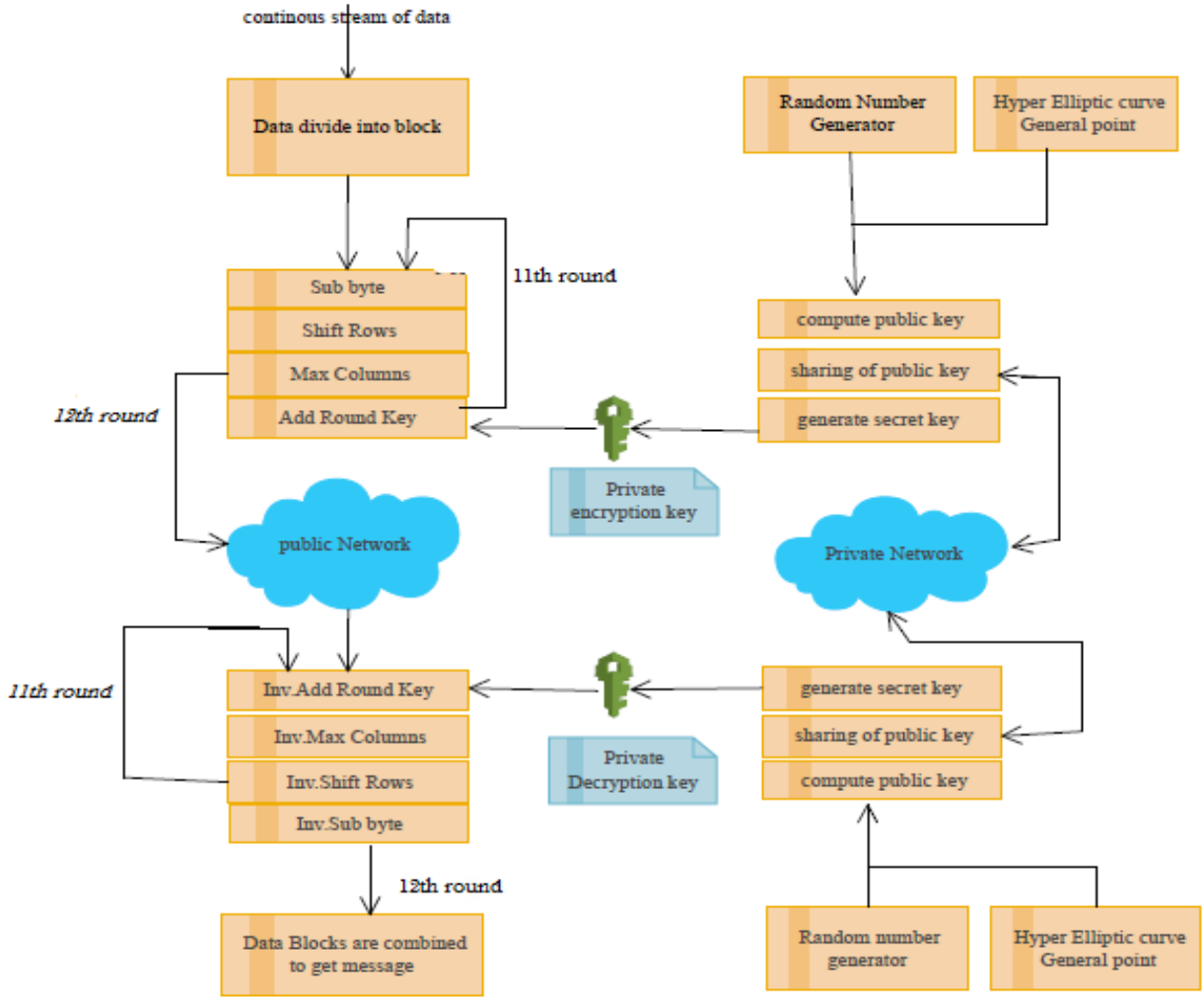

Fig. 2 Our Proposed Scheme Diagram

4. Security Analysis

The suggested scheme makes sure the authentication, confidentiality and integrity and also provides the forward and backward secrecy.

A. AUTHENTICATION

Authentication is a method by which the uniqueness of a node in a network assurances and confirms that the control or the data messages are originated from an authenticated source. In our proposed scheme the authentication IDs are preloaded to each sensor node in time of deployment in the environment. The backup of all authentication ID which are assigned to sensor nodes or also stored in a server. For first time when sensor wants to communicate with server to get

the session key for onward secure communication, sensor node sends its own authentication ID and other parameter in encrypted form to the server. Server decrypts the received data and gets the authentication of sensor. Now for node authentication server matched the received authentication ID with pre stored authentication ID, if both IDs are same, the node is legal to participate in the communication using secure session key. Otherwise it is considered illegal node and cannot participate in the communication and is also blacklisted.

B. CONFIDENTIALITLY

Confidentiality is an element of privacy that implements to protect our data from unauthorized viewers, individuals or entities. In our proposed scheme AES is used for data confidentiality and HECC is used for secure session key exchanged to protect various attacks like reply attack, main in the middle attack, masquerading attack and eavesdropping attack.

C. INTEGRITY

Integrity means the data is corrected and cannot changed during transmission form sensor node to server. Our scheme achieved integrity using one way hash function e.g. MD5.

D. FORWARD-SECRECY

Forward-secrecy is the secure data communication protocols property in which cooperation of long term keys do not cooperate previous session keys. It defends previous sessions beside upcoming concessions of secret keys. In our proposed scheme, forward secrecy is achieved using session key updating phase. In this phase after node authentication, session key will be updated for each round to send secure information from source to destination. If session key compromised in a particular round so only that round data will be effected, intruder cannot see the previous round data.

E. BACKWARD-SECRECY

Backward secrecy means that even if the current key is unprotected, the future keys cannot be properly guessed. Our proposed scheme fulfills the basic security parameter along with backward secrecy using session key update phase. If intruder compromises the session key of a particular round so it can see only that round data. Intruder cannot guess the upcoming session key for future secure communication between sensor node and server.

5. Performance Analysis

In performance analysis section we describe two types of cost communication cost and computational cost of the proposed scheme and existing scheme. We compare the proposed scheme with the existing scheme in term of quantitative analysis.

A. Computational Cost

Sensor nodes are very computational limited. The existing scheme was not suitable in wireless sensor networks. The HECC for Genus Curve g=2, g=3, g=4, g=5 and g=6 are implemented in MATLAB R2017b version. The two parameter processing time and key size are taken to test. Simulation result shows that interval occupied to generate divisor-generation, Key-generation, encryption/decryption of information. The equations Eq(b), Eq(c), Eq(d), Eq(e) and Eq(f) are executed in MATLAB.

Table 1 and table 2 show different genus computational cost for prime 35 and 55. Table 3 describes the comparison between ECC and HECC in equivalent key length of the proposed scheme and existing of the two schemes. Table 4 describes the Contrast of key size of symmetric, RSA, ECC and HECC. HECC key size is less than RSA, ECC and symmetric algorithms. Hence, the use of HECC reduces the computational cost.

Table 2: Contrast of genus g cost for size of prime 35

Method	Computational cost (ms)				
	Genus g=2	**Genus g=3**	**Genus g=4**	**Genus g=5**	**Genus g=6**
Divisor-generation	674	871	1112	1159	1177
Key-generation	2225	3347	7587	8590	11157
Encryption	3139	5182	7905	8190	8855
Decryption	3329	6207	10065	10164	11015

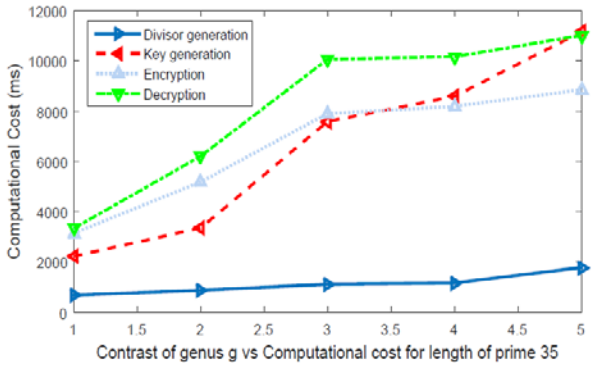

Fig. 2 Contrast of genus g vs computational cost for length of prime 35

Table 3: Contrast of genus g cost for size of prime 55

Method	Computational cost (ms)				
	Genus g=2	**Genus g=3**	**Genus g=4**	**Genus g=5**	**Genus g=6**
Divisor-generation	827	1380	1682	1912	2197
Key-generation	6791	7788	8771	11625	15585
Encryption	3139	6142	7905	8546	11503
Decryption	3329	7473	10064	10544	14261

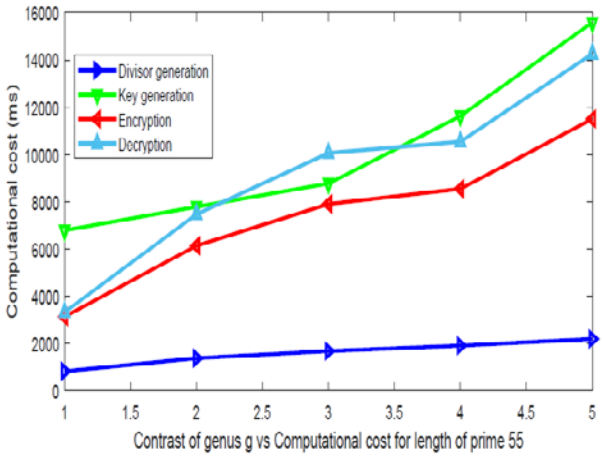

Fig. 3 Contrast of genus g vs computational cost for length of prime 55

Table 4. Contrast between ecc and hecc for equivalent key length

Scheme	Genus Curve (secrete key length)	Point Scalar Multiplication	Secret Session Key Encoding	One way MD5
Proposed scheme	HEC(80 bit key)	Two	one	One
[23]	EC(160 bit key)	Three	one	Two
[24]	EC(160 bit key)	Three	two	One

Table 5. Contrast of key size of symmetric, rsa, ecc and hecc

Symmetric key size(bits)	RSA key size(bits)	ECC key size(bits)	HECC Key size(bits)
2^{80}	2^{1024}	2^{160}	2^{80}
2^{112}	2^{2048}	2^{224}	2^{54}
2^{128}	2^{3072}	2^{256}	2^{40}

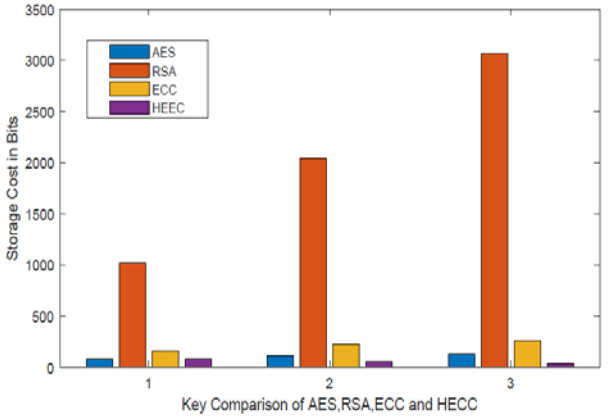

Fig .4. Key Comparison of AES, RSA, ECC and HECC

B. Communication Cost

Communication cost depends on aggregate of information. Fig 4 shows communication cost of the existing schemes and proposed scheme. When number of node is increased the communication cost will be increased. We conclude from the Fig 4, our scheme communication cost is low as compare to existing schemes [2] [9].

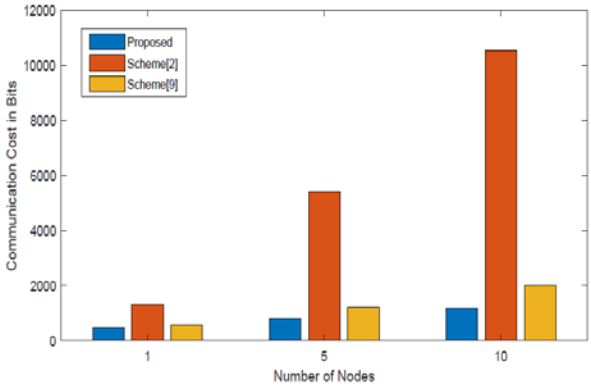

Fig. 5 Communication Cost

6. Conclusion

Due to rapid market growth and applications of WSNs, efficiency and security has become the natural demand of WSN while keeping in view its resource constrain environment. Researchers of this era have worked to ensure the secure data communication but still needed optimal and secure algorithms. In this proposed paper, we have developed an optimal and secure scheme that provides authenticity, confidentiality and integrity with the use of least resources of the system. Oure proposed scheme is manipulating the advantage of HECC and AES algorithms. We are using AES for data-encryption and data-decryption and HECC for key generation and key sharing. Our proposed algorithm is much secure with less resources and time consuming than existing algorithms.

References

[1] Zhang, S. and H. Zhang (2012). A review of wireless sensor networks and its applications. Automation and Logistics (ICAL), 2012 IEEE International Conference on, IEEE.

[2] Rizk, R. and Y. Alkady (2015). "Two-phase hybrid cryptography algorithm for wireless sensor networks." Journal of Electrical Systems and Information Technology 2(3): 296-313.

[3] He, D., S. Chan, et al. (2015). "Accountable and privacy-enhanced access control in wireless sensor networks." IEEE Transactions on Wireless Communications 14(1): 389-398.

[4] Singhal, S. and N. Singhal (2016). "A Comparative Analysis of AES and RSA Algorithms." International Journal of Scientific & Engineering Research 7(5): 149-151.

[5] Kayalvizhi, R., M. Vijayalakshmi, et al. (2010). Energy analysis of RSA and ELGAMAL algorithms for wireless sensor networks. International Conference on Network Security and Applications, Springer.

[6] Nadeem, A. and M. P. Howarth (2013). "A survey of MANET intrusion detection & prevention approaches for

network layer attacks." IEEE communications surveys & tutorials 15(4): 2027-2045.
[7] Misic, J. and V. Misic (2008). Wireless personal area networks: performance, interconnection and security with IEEE 802.15. 4, John Wiley & Sons.
[8] Sharma, S., R. K. Bansal, et al. (2013). Issues and challenges in wireless sensor networks. Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on, IEEE.
[9] Prakash, S. and A. Rajput (2018). Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks. Ambient Communications and Comput er Systems, Springer: 589-599.
[10] Biswas, K. (2014). Lightweight Security Protocol for Wireless Sensor Networks. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a, IEEE.
[11] Mary, J. R. and N. Kannammal (2017). "A Comparative Study of Security protocols in Wireless Sensor Networks."
[12] Al-Mashhadi, H. M., H. B. Abdul-Wahab, et al. (2014). Secure and time efficient hash-based message authentication algorithm for wireless sensor networks. Computer & Information Technology (GSCIT), 2014 Global Summit on, IEEE.
[13] Bhalla, M., N. Pandey, et al. (2015). Security protocols for wireless sensor networks. Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, IEEE.
[14] Panda, M. (2015). Data security in wireless sensor networks via AES algorithm. Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on, IEEE.
[15] Mani, D. and P. Nishamol (2013). "A comparison between rsa and ecc in wireless sensor networks." Int. J. Eng. Res. Technol 2: 1-5.
[16] Mahajan, P. and A. Sachdeva (2013). "A study of encryption algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology.
[17] Aleisa, N. (2015). "A Comparison of the 3DES and AES Encryption Standards." International Journal of Security and Its Applications 9(7): 241-246.
[18] Ren, W. and Z. Miao (2010). A hybrid encryption algorithm based on DES and RSA in Bluetooth communication. Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on, IEEE.
[19] Nyamasvisva, T. E. and H. Hasbullah (2010). Multi-level security algorithm for random ZigBee Wireless Sensor Networks. Information Technology (ITSim), 2010 International Symposium in, IEEE.
[20] Ajaykumar, N. and M. Sarvagya "Secure and Energy Efficient Routing Protocol in Wireless Sensor Network: A Survey.".
[21] Vijayakumar, P., V. Vijayalakshmi, et al. (2014). "Comparative study of hyperelliptic curve cryptosystem over prime field and its Survey." International Journal of Hybrid Information Technology 7(1): 137-146.
[22] Zargar, A. J., M. Manzoor, et al. (2017). "ENCRYPTION/DECRYPTION USING ELLIPTICAL CURVE CRYPTOGRAPHY." International Journal of Advanced Research in Computer Science 8(7).
[23] Gupta, D., A. De, et al. (2012). "Performance study of genus 3 hyperelliptic curve cryptosystem." Journal of Information Processing Systems 8(1): 145-158.
[24] Aydos, M., T. Yanık, et al. (2001). "High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor." IEE Proceedings-Communications 148(5): 273-279.

Irshad Ullah was born on April 7, 1993 in Dir (Lower), Khyber Pakhtunkhwa (KPK), Pakistan. He received the BS (Hons) in Computer Science degree from Institute of Information Technology (IIT), Kohat University of Science and Technology (KUST), Pakistan in 2016. He is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. His research interest includes secure communication in Wireless Sensor Networks, Vehicular ad hoc networks (VANETs) and Smart Grid. (E-mail: irshadullah136@gmail.com)

Dr. Noor Ul Amin is Head Department of Telecommunication at Hazara University Mansehra. He completed his MSc in Computer Science at University of Peshawar in 1996 and his MS and PhD in Computer Sciences at International Islamic University Islamabad, Hazara University Mansehra subsequently. He has recently completed R & D project sponsored by Ministry of Science and Technology, Pakistan. He has been the session chair in the IEEE and Springer conferences. His research interests include Information Security, Wireless Sensor Networks, Steganography and Information-Centric Networking. He has authored more than 80 peer-reviewed journals articles and conference proceedings. (E-mail: namin@hu.edu.pk)

Mr. Jawaid Iqbal received the BS (Computer Science) degree from Institute of Business and Management Sciences (IBMS), Agriculture University Peshawar in 2010. He obtained the MS (Computer Science) degree with grade very good with honor from Department of Information Technology, Hazara University. Mansehra, K-P, Pakistan. He is currently PhD Scholar (Computer Science) at Department of Information Technology, Hazara University Mansehra, Pakistan. He is currently Lecturer in Department of information technology, Hazara University Mansehra Pakistan.
He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2012 up to till date. He believe in quality research in the area of Cryptography, Information and Networks Security. He is currently active in Elliptic/Hyper Elliptic Curve Cryptography, Signcryption, Sensor Networks, Smart Grid and VANT Security. PhD thesis focused on secure communication of

sensitive information in Wireless Body Area Networks (WBANs). (E-mail: jawaid5825@gmail.com)

Muhammad Shahid received the BCS degree form Peshawar University Pakistan in 2014. He obtained the MCS degree from Hazara University Mansehra, Pakistan in 2017. He is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. His research interest includes Information Security and Cryptography.(E-mail: mshahidkhan32@gmail.com)

Farman Ali received the BS (Hons) in Computer Science degree from Hazara University Mansehra, Pakistan in 2016. He is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. His research interest includes security of Wireless Body Area Networks (WBANs). (E-mail: akhundzai@gmail.com)