International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 10 No. 1 Oct. 2014, pp. 6-18

http://www.ijisr.issr-journals.org/

An Efficient Blind Signature Authentication for Wireless Sensor Networks Using HECC

T. Gomathi, V. Manju, and N. Anuradha

Department of ETCE,
Sathyabama University,
Chennai, Tamilnadu, India

ABSTRACT: The challenging issue in the design and deployment of Wireless Sensor Networks (WSNs) is the key management and authentication scheme due to the constraints in the sensor networks. The major constraints in Wireless Sensor Networks are large memory storage, more computational complexity and limited resource. Hence, in order to overcome these constraints and to achieve secure communication between sensor nodes, it is important to establish an efficient key predistribution mechanism. Inspite of the fact that many elegant and clever solutions have been proposed, no practical efficient key predistribution has emerged. The existing key management scheme in WSN using ECC provides a predistribution scheme with bigger key sizes and increased memory overhead. The computational complexity is also high which increases the processing time. The recent progress and research on HECC provides new opportunities to utilize public-key cryptography in Wireless Sensor Networks. The key generation for HECC polynomial using genus-2 curve was performed. The encryption and decryption algorithm for HECC was formulated. The key predistribution using HECC and ECC were implemented in wireless sensor network and simulated using NS2 simulator. The various performance analysis namely delay, throughput and power for both HECC and ECC were performed and the results are shown. It is inferred from the results that the proposed HECC scheme outperforms the existing ECC scheme. Further in this project work, the Blind Signature using HECC and Digital Signature using HECC has been implemented in WSN using NS2. The various performance metrics for both the signature schemes have been obtained and the results were compared.

KEYWORDS: WSN, Key predistribution, HECC, ECC, DS, BS.

1 INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The major constraints in WSN are power consumption, memory, computational capability. Hence the appropriate encryption scheme should be selected considering these considerations. If more security is needed for some applications then accordingly the encryption algorithm has to be selected.

1.1 PUBLIC KEY CRYPTOGRAPHY

Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristics: It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key. One of the first approach to public key encryption is the RSA scheme. It is the most widely accepted and implemented general purpose approach to public- key encryption. The key length for secure RSA has been increasing and this put a heavier processing load on applications using RSA. This burden has

Corresponding Author: T. Gomathi

ramifications especially for electronic commerce sites that conduct large numbers of secure transactions. Recently a competing system has begun to challenge RSA: Elliptic curve cryptography (ECC).

The principle attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead. Thus there is a computational advantage of using ECC with a shorter key length than a comparably secure RSA. The key length of ECC is 120 bits. Cryptanalysts have founded Hyper Elliptic Curve Cryptography which is also a public key cryptography whose key length is very much lesser than that of Elliptic Curve Cryptography (ECC).The key length of HECC is 80 bits. Hence by reducing the key length the computational time is decreased, which in turn increases the processing speed that leads to increased throughput. [1]

1.2 KEY DISTRIBUTION SCHEME

Key distribution is an important issue in wireless sensor network (WSN) design. It is a newly developing field due to the recent improvements in wireless communications. Key predistribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position. Key predistribution schemes are various methods that have been developed by academicians for a better maintenance of key management in WSNs. Basically a key predistribution scheme has 3 phases:

- Key distribution
- Shared key discovery
- Path-key establishment

During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key predistribution scheme used in creation.

The paper is organized as follows: Section II gives an idea about the existing scheme, Section III deals with the proposed key predistribution scheme. Section IV discusses th performance analysis and comparison of existing and proposed key predistribution. Section v deals with the conclusion

2 EXISTING SCHEME

The existing key predistribution uses ECC in wireless sensor networks.ECC is also a public key cryptography .This encryption algorithm has been implemented on WSN. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. ECC devices require less storage, less power, less memory, and less bandwidth than other systems. This allows us to implement cryptography in platforms that are constrained, such as wireless devices, handheld computers, smart cards, and thin-clients.

3 PROPOSED SCHEME

To overcome the above limitations, this project work proposes an efficient key predistribution scheme which establishes shared keys between sensor nodes using Hyper Elliptic Curve Cryptography (HECC) in WSN. By this proposed method, greater security, stronger resilience, low energy consumption and less memory storage can be achieved. HECC is a typical fast public key cryptosystem with high efficiency and security. Hyper Elliptic Curve Cryptosystem [2],[3]is the natural generalization of Elliptic curve Cryptosystem. In HECC a secure Jacobian group with large prime number order can be constructed on a relatively smaller basic field. HECC can acquire the same security level with shorter operating parameters. If the basic finite field is 60 bits, the security level of HECC is equivalent to that of Elliptic Curve Cryptography with 180 bits, and it is far secured than RSA with1024 bits. In cryptography a blind signature as introduced by David Chaum, is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, 7nblended message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

The recent progress and research on HECC provides new opportunities to utilize public-key cryptography in Wireless Sensor Networks. The key generation for HECC polynomial using genus-2 curve was performed.

3.1 KEY PREDISTRIBUTION IN WSN USING HECC

The key predistribution in WSN is done using HECC [4],[5]. The private key and identity are given to each and every sensor nodes during manufacturing process itself. Whenever nodes want to communicate between each other then the server will give a key for that particular session to those nodes. With the help of that session key and their private keys , the nodes will generate the secret common key for them to establish communication. Thus by using the common secret key the nodes can communicate the message securely.The algorithm for generating the public and private key generation for HECC is as follows:

Step 1: Select a hyper elliptic curve C, prime number p and divisor D.
Step 2: Choose a prime random number a_A that belongs to a group N.
Step 3: Generate the public key $P_{A =} a_A$ * D.
Step 4: Return the public key P_A and the private key a_A.

3.2 DIGITAL SIGNATURE

A digital signature [6],[7] is an electronic signature used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. It can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. Digital Signature Certificates [8], [9], [10] can be used for eFiling of Income Tax Returns, eTendering in India on Government Websites such as Indian Railway

4 PERFORMANCE ANALYSIS OF EXISTING SCHEME

The performance characteristics of the proposed scheme and the existing scheme were simulated and compared. The various performance metrics namely delay, throughput and power consumption are analyzed for the proposed scheme and the existing scheme. The proposed algorithm ensures successful data delivery, less delay, greater throughput, optimal power consumption and increased efficiency. The simulation is performed using Network Simulator 2 (NS2) software.

The Elliptic Curve Cryptography is implemented in WSN and its various performance metrics namely delay, throughput and power are calculated. The results are tabulated and discussed.

4.1 AVERAGE DELAY ANALYSIS FOR ECC

The simulation result of average delay analysis is shown in Figure 1 for ECC. It is inferred from the graph that the average delay for each and every node is very high and it ranges in the range of 19 ms. The reason is that the computational time for the existing scheme is very high which in turn increases the delay.

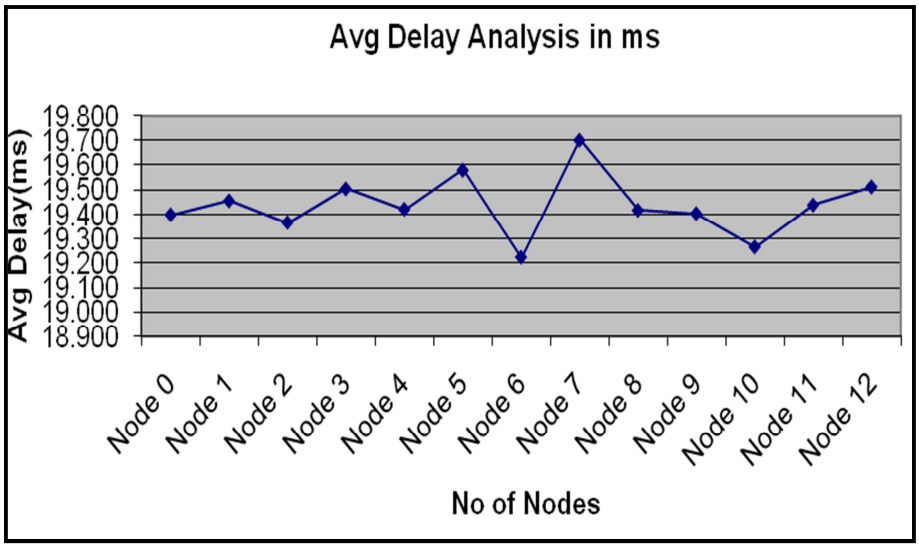

Fig.1 Average Delay Analysis for ECC

4.2 AVERAGE THROUGHPUT ANALYSIS FOR ECC

The simulation result of average throughput analysis is shown in Fig 2 for ECC. The graph shows that the throughput in each and every node is low for the proposed scheme. The throughput for each node is in the range of 77 % for ECC. Hence there is a lesser throughput because of more delay. Thus the computational time is increased which in turn reduces the throughput for the existing ECC scheme.

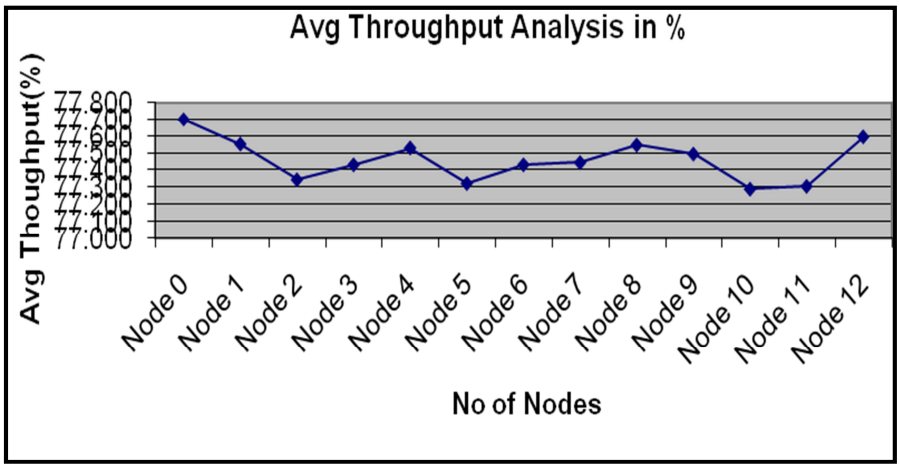

Fig. 2 Average Throughput analysis for ECC

4.3 AVERAGE POWER ANALYSIS FOR ECC

The simulation result of average power analysis is shown in Fig 3 for ECC. The graph shows that the power consumed by each and every node is more for the proposed scheme. The power is the major constraint in case of sensor networks. If a scheme consumes more power then it will not be an optimal scheme for implementing in WSN. The power consumed by each node for the existing Elliptic Curve Cryptography is in the range of 257mW.

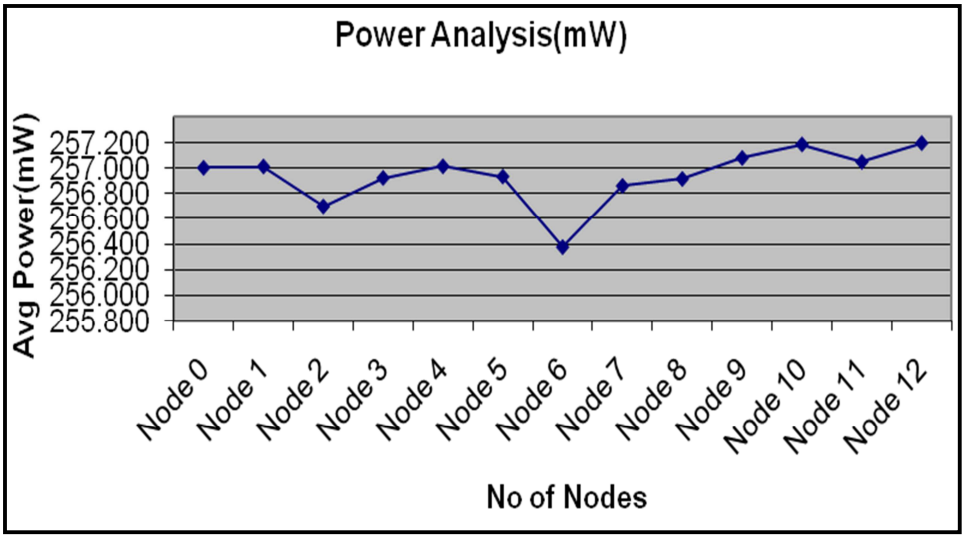

Fig. 3 Average Power for ECC

5 PERFORMANCE ANALYSIS OF PROPOSED SCHEME IN WSN

Genus 2 Jacobian hyper elliptic curve has been taken and implemented in WSN. The various metrics are analyzed for the proposed HECC scheme. The results are tabulated and discussed.

5.1 AVERAGE DELAY ANALYSIS FOR HECC

The simulation result of average delay analysis is shown in Fig 4 for HECC. It is inferred from the graph that the average delay for each and every node is very less and it ranges in the range of 11 ms. The reason is that the computational time for the proposed scheme is very less which in turn reduces the delay.

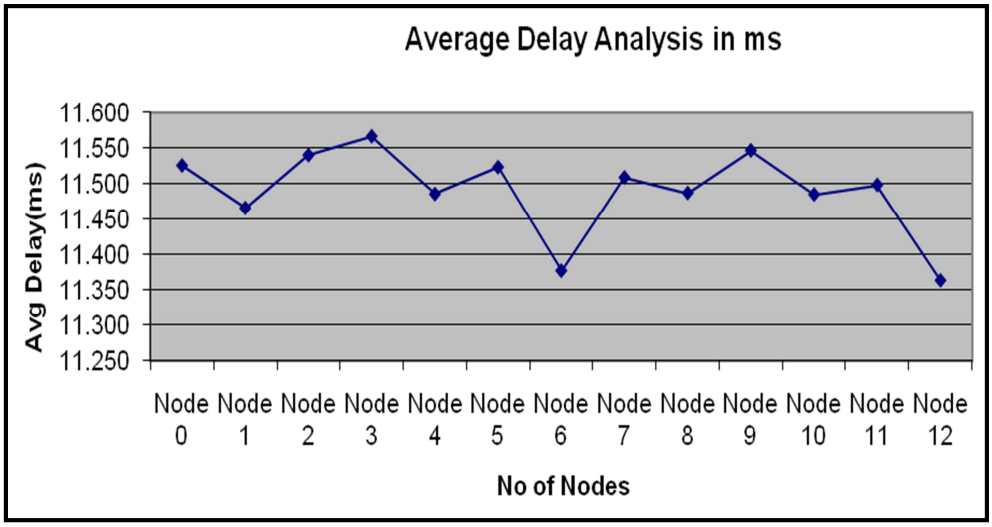

Fig. 4 Average Delay Analysis for HECC

5.2 AVERAGE THROUGHPUT ANALYSIS FOR HECC

The simulation result of average throughput analysis is shown in Fig.5 for HECC. The graph shows that the throughput in each and every node is high for the proposed scheme. The throughput for each node is in the range of 87 % for HECC. Hence there is a greater throughput because of lesser delay. Thus by reducing the computational time the throughput is increased for the proposed HECC scheme.

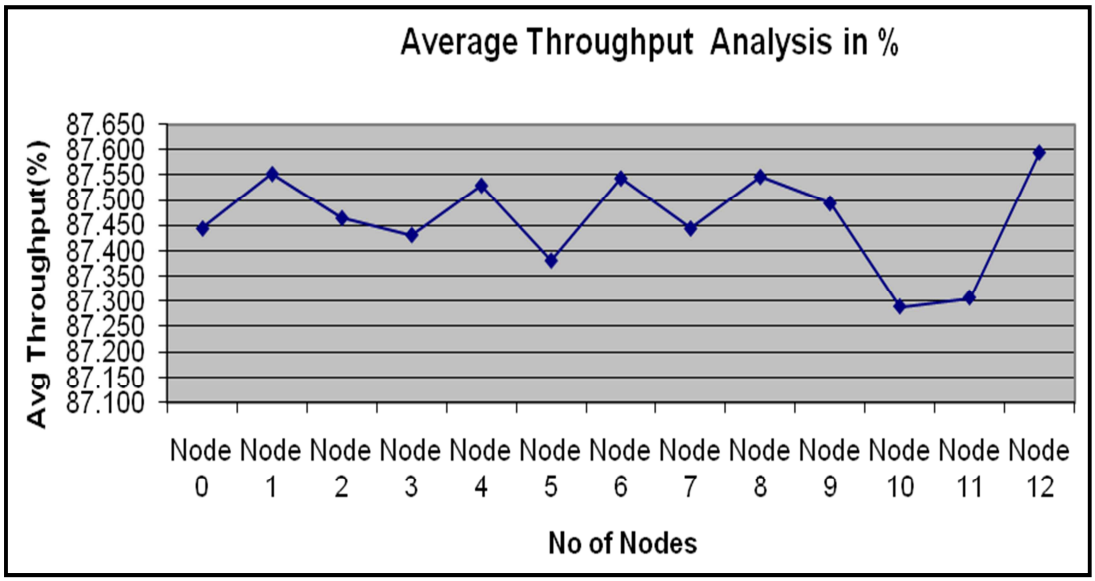

Fig.5 Average Throughput Analysis for HECC

5.3 AVERAGE POWER ANALYSIS FOR HECC

The simulation result of average power analysis is shown in Fig 6 for HECC. The graph shows that the power consumed by each and every node is less for the proposed scheme. The power is the major constraint in case of sensor networks. If a

scheme consumes less power then it will be definitely an optimal scheme that can be used in WSN. The power consumed by each node for the proposed Hyper Elliptic Curve Cryptography is in the range of 248mW.

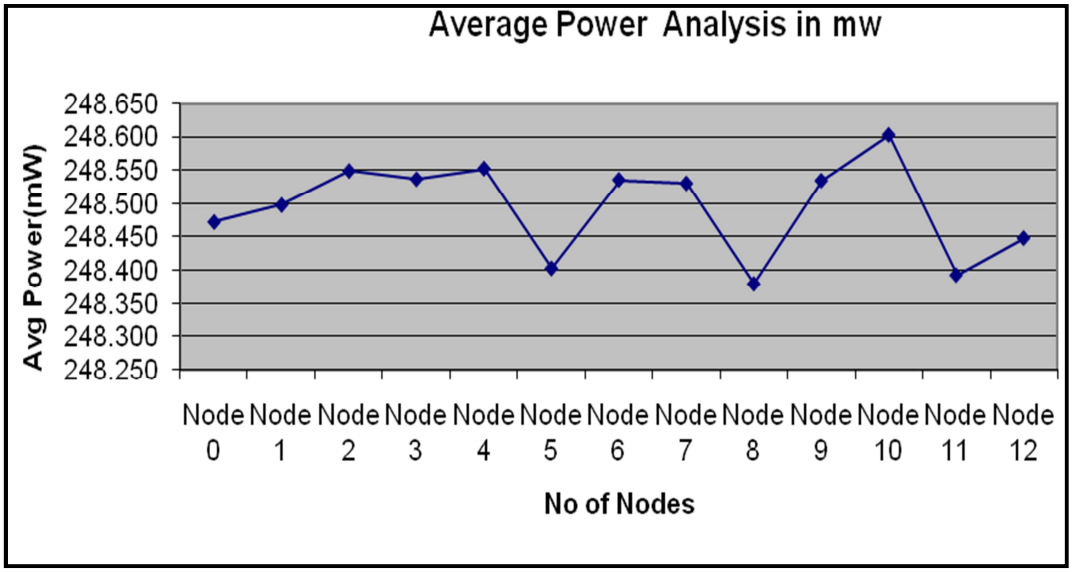

Fig. 6 Average Power for HECC

5.4 COMPARISON OF HECC AND ECC

The performance analysis of both the existing HECC and the proposed ECC schemes are compared and their performance metrics are analyzed. The parameters namely delay, throughput and power are compared for both the schemes. The results are tabulated and discussed.

5.4.1 DELAY ANALYSIS COMPARISON OF HECC AND ECC

The simulated result for delay analysis comparison is shown in Figure 4.7 for the existing and the proposed scheme. It is inferred from the graph that the delay is more in the existing Elliptic Curve Cryptographic scheme than the proposed Hyper Elliptic Curve Cryptographic scheme.

The delay is in the range of 11ms for HECC and for ECC the delay is in the range of 19ms.It is inferred from the graph that the computational time increases which in turn increases the delay for the existing scheme whereas the computational time is less which decreases the delay for the proposed scheme.

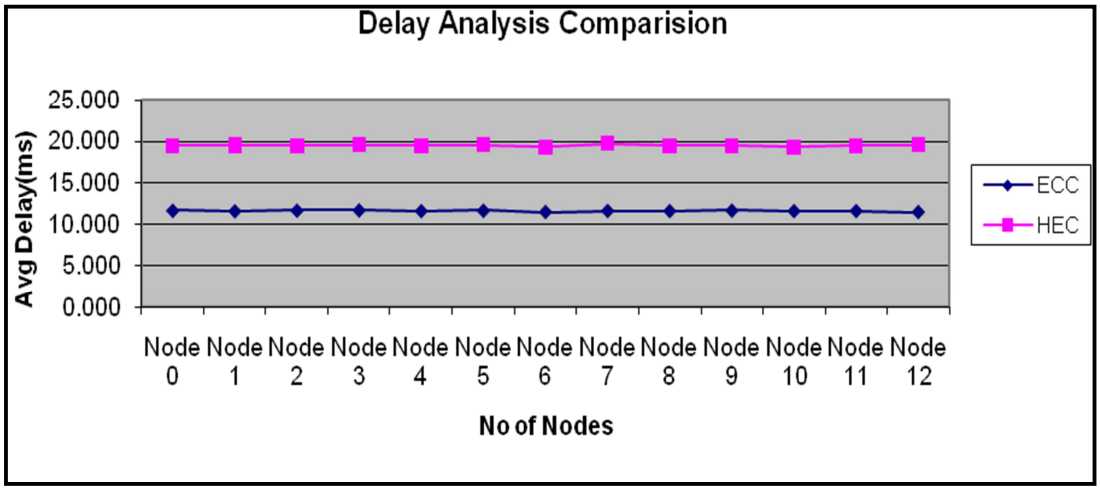

Fig. 7 Delay Analysis Comparison of HECC and ECC

5.4.2 THROUGHPUT ANALYSIS COMPARISON OF HECC AND ECC

The simulated result for throughput analysis comparison is shown in Figure 4.8 for the existing and the proposed scheme. It is inferred from the graph that the throughput is lesser in the existing Elliptic Curve Cryptographic scheme than the proposed Hyper Elliptic Curve Cryptographic scheme. The throughput is in the range of 87% for HECC and for ECC the throughput is in the range of 77%.It is inferred from the graph that the computational time increases which in turn decreases the throughput for the existing scheme whereas the computational time is less which increases the throughput for the proposed scheme.

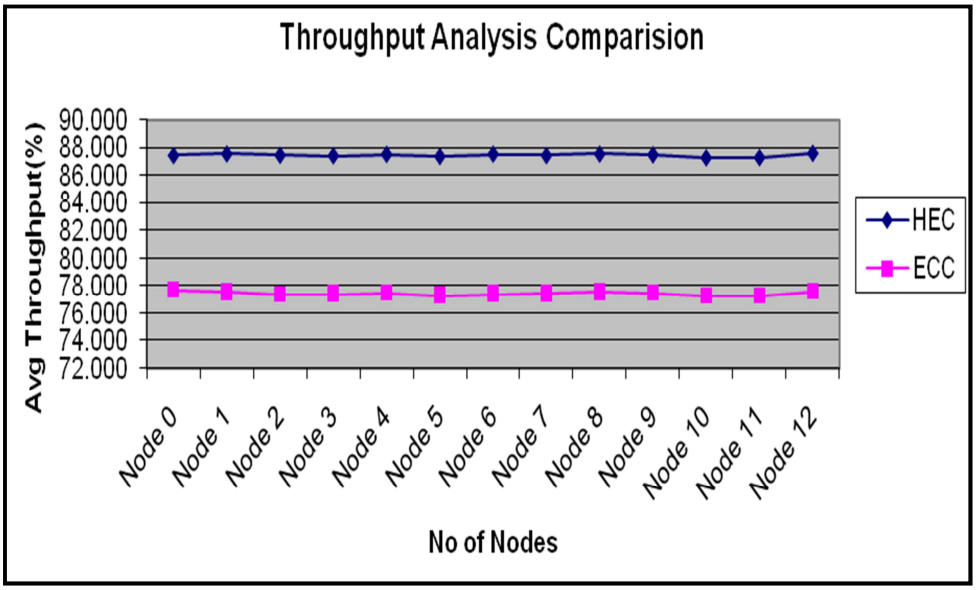

Fig. 8 Throughput Analysis Comparison of HECC and ECC

5.4.3 POWER ANALYSIS COMPARISON OF HECC AND ECC

The simulated result for power analysis comparison is shown in Figure 4.9 for the existing and the proposed scheme. It is inferred from the graph that the energy consumed is more in the existing Elliptic Curve Cryptographic scheme than the proposed Hyper Elliptic Curve Cryptographic scheme. The power is in the range of 248 for HECC and for ECC the throughput is in the range of 257Mw. It is inferred from the graph that the computational time increases which in turn increases the power consumption for the existing scheme whereas the computational time is less which decreases the power consumption for the proposed scheme. Thus the proposed scheme is optimal that can be implemented in WSN more efficiently and effectively.

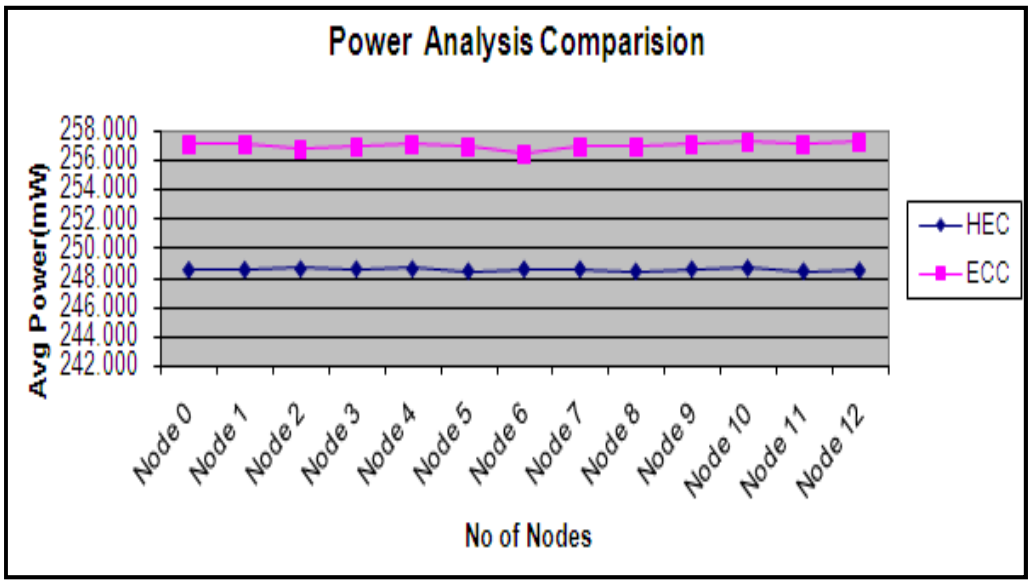

Fig. 9 Power Analysis Comparison of HECC and ECC

6 PERFORMANCE ANALYSIS OF DIGITAL SIGNATURE USING HECC

Digital Signature (DS) using HECC is implemented in WSN and its various performance metrics namely signing time, verification time, packet loss and throughput are calculated. The results are tabulated and discussed.

The simulation result of average signing time analysis is shown in Fig 10 for Digital Signature. It is inferred from the graph that the maximum average signing time for a node is very high and it ranges in the range of 1.59 sec. The reason is that the signing time is very high which in turn increases the delay.

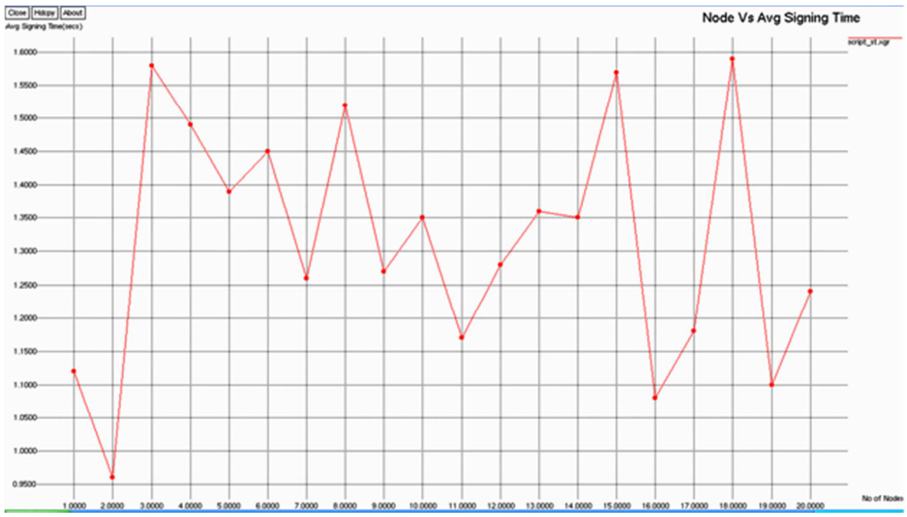

Fig 10 Average Signing Time Analysis for DS

6.1 AVERAGE VERIFICATION TIME ANALYSIS FOR DS

The simulation result of average verification analysis is shown in Fig 11 for Digital Signature. The graph shows that the average verification time for each and every node varies between 1.3 sec and 1.62 sec for the existing scheme. Hence there is a lesser throughput because of more delay. Thus the computational time is increased which in turn reduces the throughput for the existing digital signature scheme.

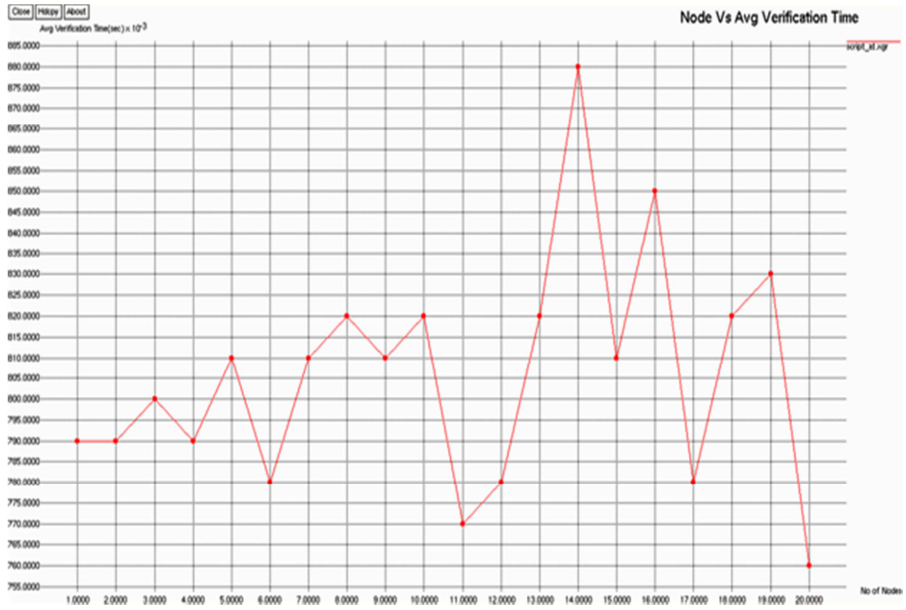

Fig 11 Average Verification Time Analysis for DS

6.2 AVERAGE PACKET LOSS ANALYSIS FOR DS

The simulation result of average packet analysis is shown in Fig 12 for digital signature using HECC. The graph shows that the packet loss for each and every node varies between 15.5 % and 19.5 % for the existing scheme. The signing time and verification time for the existing scheme is more which in turn increases the packet loss.

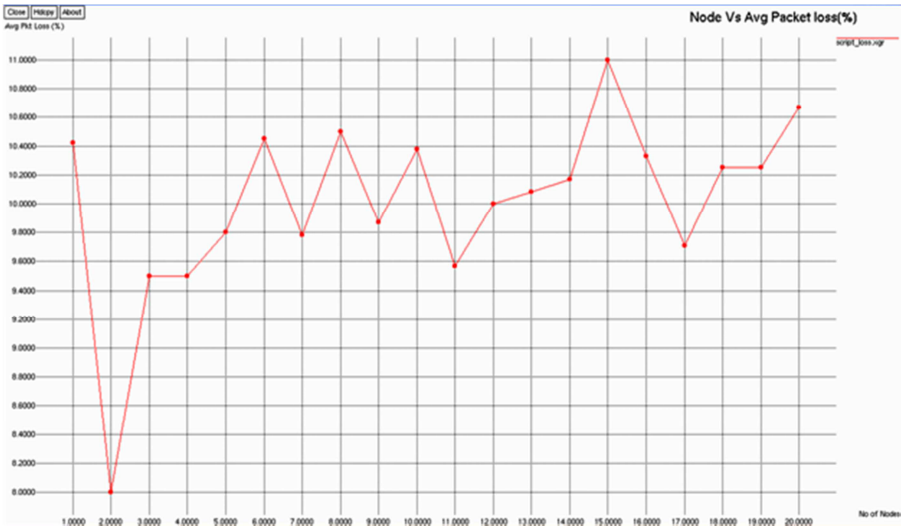

Fig 12 Average Packet Loss Analysis for DS

6.3 AVERAGE THROUGHPUT ANALYSIS FOR DIGITAL SIGNATURE

The simulation result of average throughput analysis is shown in Fig 13 for the existing digital signature. The graph shows that the throughput at each and every node is less for the existing scheme. The throughput at each node for the existing digital signature is in the range of 73 % to 79%.

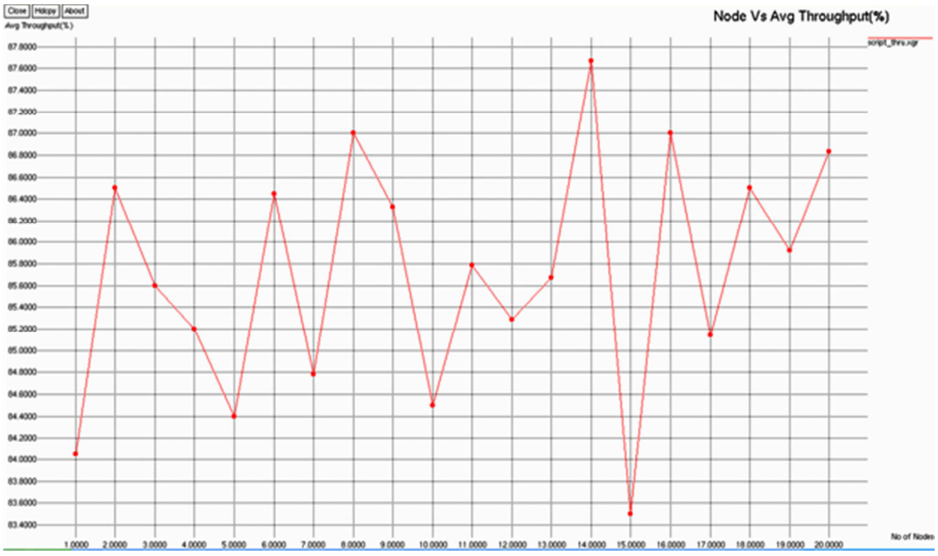

Fig 13 Average Throughput Analysis for DS

7 PERFORMANCE ANALYSIS OF BLIND SIGNATURE USING HECC

Genus 2 Jacobian hyper elliptic curve has been taken and implemented in WSN. The various metrics are analyzed for the proposed Blind Signature (BS) authentication scheme. The results are tabulated and discussed.

7.1 AVERAGE SIGNING TIME ANALYSIS FOR BS

The simulation result of average delay analysis is shown in Fig 14 for blind signature using HECC. It is inferred from the graph that the average delay for each and every node is very less and it ranges between 0.66 sec and 0.88 sec. The reason is that the signing time for the proposed scheme is very less which in turn reduces the delay.

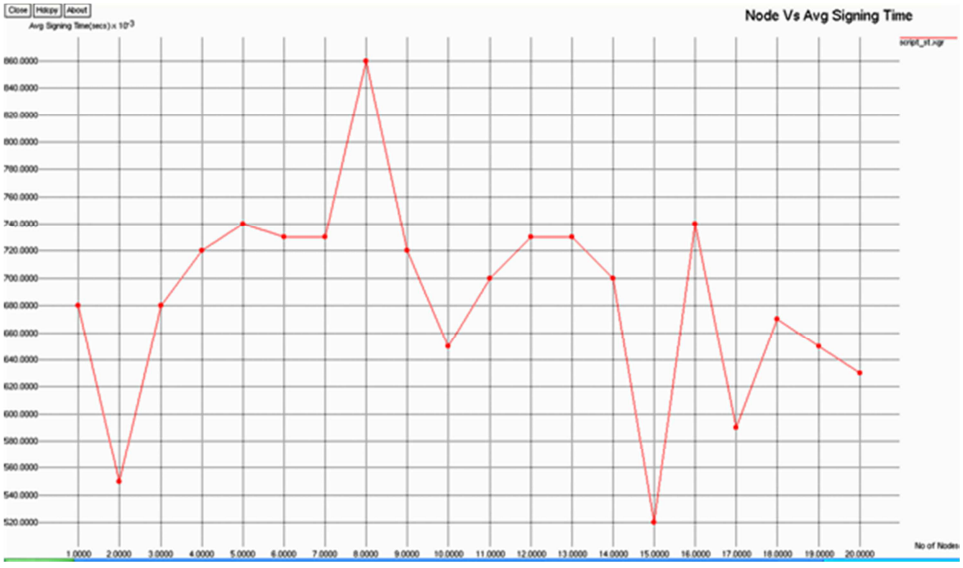

Fig 14 Average Signing Time Analysis for BS

7.2 AVERAGE VERIFICATION TIME ANALYSIS FOR BLIND SIGNATURE

The simulation result of average verification time analysis is shown in Fig 15 for blind signature using HECC. The graph shows that the verification time for each and every node is less for the proposed scheme. The verification time for each node

varies between 0.76 sec and 0.88 sec for the proposed scheme. Hence there is a greater throughput because of lesser delay. Thus by reducing the verification time the throughput is increased for the proposed Blind Signature scheme.

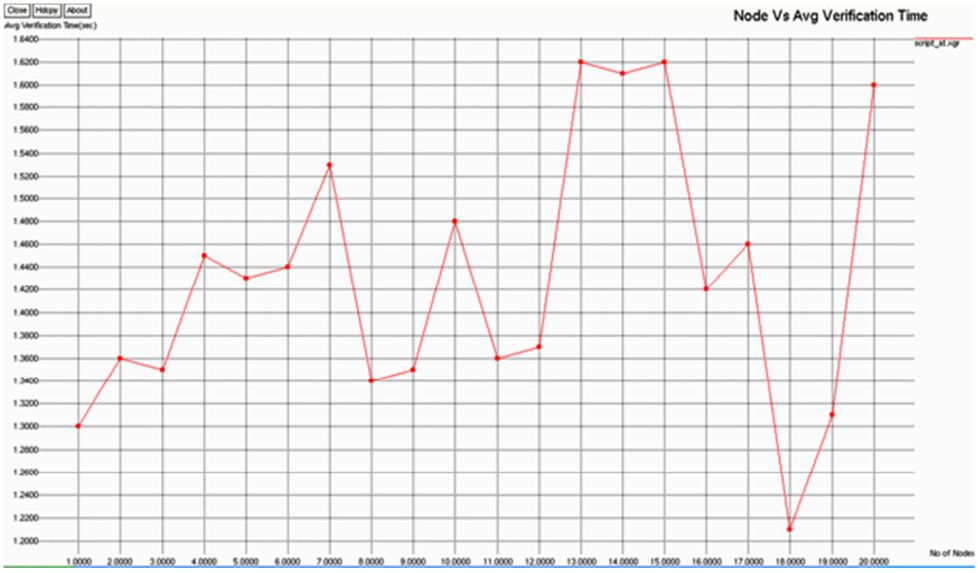

Fig 15 Average Verification Time Analysis for BS

7.3 AVERAGE PACKET LOSS ANALYSIS FOR BS

The simulation result of average packet loss analysis is shown in Fig 16 for blind signature using HECC. The graph shows that the packet loss at each and every node is less for the proposed scheme. Since the signing time and verification time are optimal for the proposed scheme the delay will be less which in turn reduces the packet loss. The packet loss for each node varies between 10.4% and 11%.

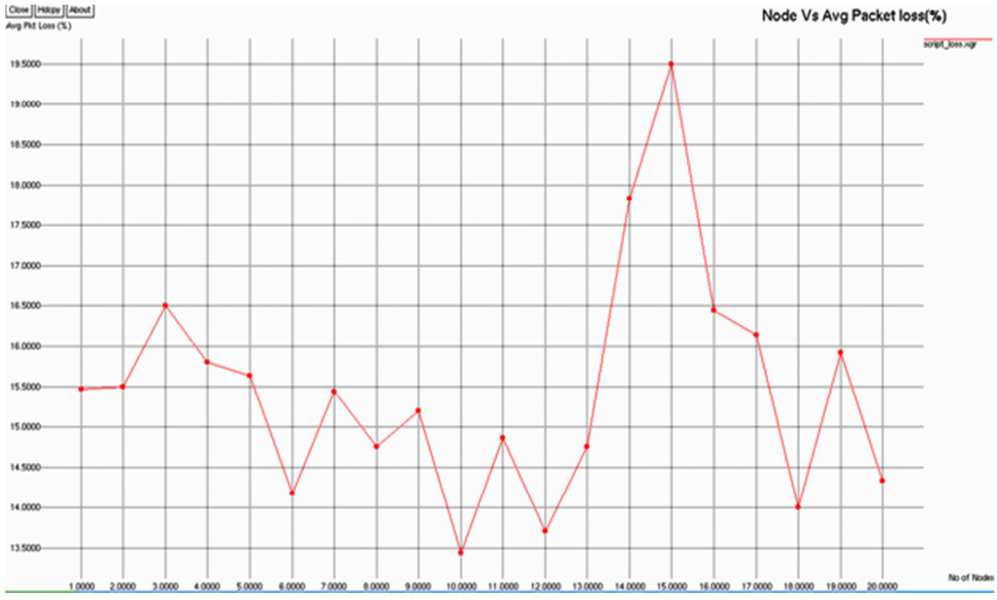

Fig 16 Average Packet Loss Analysis for BS

7.4 AVERAGE THROUGHPUT ANALYSIS FOR BS

The simulation result of average throughput analysis is shown in Fig 17 for blind signature using HECC. The graph shows that the throughput for each and every node is greater for the proposed scheme. The signing time and verification time are optimal for the proposed blind signature scheme using HECC in WSN which in turn increases the throughput for the proposed scheme. The throughput ranges between 83 % and 87.8 %.

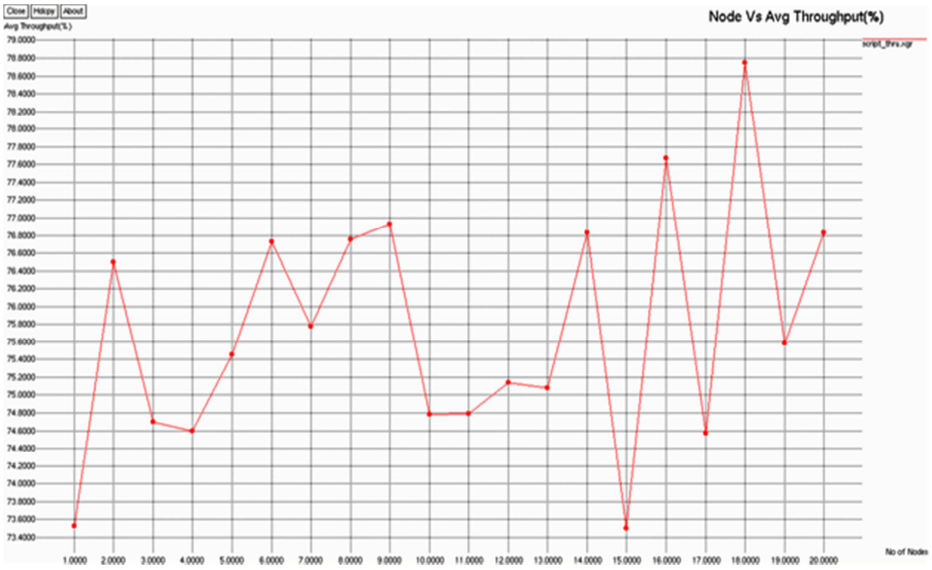

Fig 17 Average Throughput Analysis for BS

7.5 COMPARISON TABULAR COLUMN OF BOTH BS AND DS

The performance analysis of the proposed and the existing scheme is given in Table 3.The various performance metrics namely signing time, verification time, packet loss and throughput of both the schemes are tabulated herewith. The signing and verification time for each and every node is lesser for blind signature than digital signature. Hence the throughput is better for the proposed HECC blind signature in WSN. The packet loss is lesser for the proposed authentication scheme.

Table 1. Comparison of Performance Analysis for BS and DS

NO	PERFORMANCE METRICS	PROPOSED BS SCHEME	EXISTING DS SCHEME	PERCENTAGE OF SAVING BY THE PROPOSED SCHEME
1.	A Average Signing Time	0.66 Sec	1.58 Sec	0.92 sec
2.	Average Verification Time	0.88 Sec	1.62 Sec	0.74 sec
3.	Packet Loss	11 %	19.5 %	8.5 %
4.	Average Throughput	87.8 %	78.8 %	9 %

8 CONCLUSION

An efficient key predistribution and authentication scheme is proposed for wireless sensor networks considering the constraints in WSN. The proposed scheme using genus 2 curve Hyper Elliptic Curve Cryptography has been implemented in wireless sensor network which decreases the computational time thereby increasing the throughput.

The power consumption is a major constraint in case of wireless sensor networks. Thus the proposed scheme reduces the power consumption in WSN. The various performance analysis namely delay, throughput and power consumption have been analyzed and compared with the existing Elliptic Curve Cryptography scheme. The delay is more in the existing scheme. Hence the computational time is also more which leads to reduction in the throughput. It also consumes more power than the proposed scheme.

Thus the proposed scheme provides a better performance which has greater throughput, lesser delay and efficient utilization of power. There is a proportionate increase in throughput by 10% for HECC than the existing scheme. The delay reduces greatly by 8ms and the average power consumed by HECC is reduced by 10 mW. It is inferred from the results that the proposed HECC scheme outperforms the existing ECC scheme. The various performance analysis namely signing time, verification time, packet loss and throughput have been analyzed and compared with the existing authentication scheme. The delay is more in the existing scheme which in turn increases the packet loss also. The computational time for the existing scheme is also more which leads to reduction in the throughput. It also consumes more time for signing and verification than the proposed scheme.

The analysis of the proposed blind signature using Hyper Elliptic Curve has shown that the throughput of the scheme has been increased by decreasing the signing time and verification time. Since the signing and verification time is less there is an efficient usage of energy. The existing scheme has more delay which reduces the throughput to a greater extent which has been overcome by the proposed scheme. There is a decrease in the average signing time and verification time by 0.92 sec and 0.74 sec respectively. The throughput shows an increase by 9 % for the proposed scheme than the existing scheme. There is a proportional reduction in verification time by for the proposed scheme. The appropriate inferences pertaining to the results were discussed. It is inferred from the results that the proposed blind signature using HECC scheme outperforms the existing digital signature HECC scheme.

9 SCOPE OF FUTURE WORK

The main contribution of this project is the implementation of key predistribution scheme and authentication by a proposed algorithm using genus 2 curve. Further work is to propose an efficient ID-based partially blind signature scheme for mobile e-commerce applications in order to improve efficiency and to reduce the computational time by the usage of genus 3 and genus 4 curves. Methods to analyze the higher degree curves have to be developed. In this case, these methods should be capable of decreasing the computational time, delay and power consumption.

REFERENCES

[1] Qing Chang, Yong-ping ZHANG, Lin-lin Qin, "A Node Authentication Protocol based on ECC in WSN," International *Conference on Computer Design and Applications (ICCDA 2010)*, vol. 20, no. 6, August 2010.

[2] Nivethaa Shree.K and Dr.Latha Parthiban, "Knapsack-Based Elliptic Curve Cryptography Using Stern Series for Digital Signature Authentication," *International Conference on* E*merging Trends in Electrical and Computer Technology (ICETECT),*vol. 12, no. 1, March 2011.

[3] Deng Jian-zhi, Cheng Xiao-hui, and Gui Qiong, "Design of Hyper Elliptic Curve Digital Signature, " International Conference on Information Technology and Computer Science, vol. 2 , no. 3, pp. 45-47, July 2009.

[4] Nizamuddin, Shehzad Ashraf Ch., Waqas Nasar, and Qaisar Javaid, "Efficient Signcryption Schemes based on Hyperelliptic Curve Cryptosystem," *Journal on Applied Mechanics and Materials*, vol.1, no.7, pp. 546 – 552, September 2011.

[5] Xuanwu and Zhou, "Improved Ring Signature Scheme Based on Hyper-elliptic Curves, " *Second International Conference on Future Information Technology and Management Engineering,* vol. 3, no. 2, pp. 373- 376, December 2009.

[6] Dae Hyun Yum, Jin Seok Kim, Sung Je Hong, and Pil Joong Lee, "Distance Bounding Protocol for Mutual Authentication, " *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, February 2011.

[7] Lein Harn and Jian Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, July 2011

[8] Xuanwu Zhou and Xiaoyuan Yang, "Hyper-elliptic Curves Cryptosystem Based Blind Signature," IEEE *Transactions Wireless Communication,* vol. 9, pp. 168-174, January 2009.

[9] Caimu Tang, *Member, Dapeng Oliver Wu,* Anthony T. Chronopoulos *and Cauligi S. Raghavendra,* "Efficient Multi-Party Digital Signature using Adaptive Secret Sharing for Low-Power Devices in Wireless Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, Feb. 2009.

[10] Manik Lal Das, "Two-Factor User Authentication in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, March 2009.