IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

Multi Level Identity based Cryptography for Improved Security in WSN

Prof. Bachala Sathyanarayana [1], P. Sumalatha [2]

[1] Professor , Department of Computer Science and Technology,
Sri Krishnadevaraya University,Anantapuramu,

[2] Research Scholar, Department of Computer Science and Technology,
Sri Krishnadevaraya University,Anantapuramu,

ABSTRACT

Ever since Shamir proposed Identity Based Signature there has been considerable research in improving Identity Based Cryptography for providing security to Wireless Sensor Network communications. IBC could eliminate costly third party certificates and verification process of its predecessor besides making key management simple. With IBC it is possible to use any publicly known identity to generate security keys so as to make it intuitive. In our previous work, we enhanced IBC for efficient key management and applied it to group key management. In this paper we proposed Multi-level Identity Based Cryptography (MIBC) for the first time and explored its utility in maximizing security in WSN. Precisely, the multi-level identity based cryptography proposed by us can be used for secure digital authentication which brings about high level of system security. Our extensive simulations reveal that the proposed scheme is flexible, scalable and provide high level of security to communications in WSN.

Indexed Terms – WSN, security, multi-level IBC, cryptography, digital signature

1. INTRODUCTION

Identity Based signature scheme was first introduced by Shamir in 1984 [2]. However, Shamir covered only the signature part of the scheme for securing systems. Later on in 2001, Boneh and Franklin [3] enhanced the scheme of Shamir and applied Identity Based Cryptogrpahy (IBC) for efficient key management that involves encryption and decryption. It was an extended model to Public Key Infrastructure (PKI). Taking the work of Boneh and Franklin as basis Nicanfar and Leung [4] proposed a conceptual design of Enhanced Identity Based Cryptography (EIBC). The EIBC could minimize control packets involved in the key management and resulted in significant improvement in optimizing resource utilization. Our work in [1] was based on the work of Nicanfar and Leung where we adapted EIBC for multicast group key management in WSN. In this paper we extend it further to make it a multi-level identity based cryptography scheme for more robust, flexible and secure communications in WSN. We conceived the concept of multi-level identity based cryptography in our survey of literature [5]. To our knowledge, this is for the first time an IBC is enhanced to have multi-level identity based cryptography. A good survey of existing IBC schemes can be found in [6].

Earlier IBC was enhanced by many researchers using Elliptic Curve Cryptography (ECC). Hierarchical ID-Based Cryptogrphy (HIDBC) was explored in [7]. Later the HIDBC was applied to grid security by Lim *et al*. [8]. The IBC and ECC were used by Menezes [8] for pairing based cryptography. The basic concepts of IBC including design, feasibility, bilinear pairing, criteria for deployment and signatures based on IBC are found in [9]. Nicanfar and Leung applied IBC for two real world applications such as utility network for smart grid communications [10] and for high security communications in home area networks [11].

Contribution: Our contribution in this paper is improvement of enhanced identity based cryptography scheme explored in our previous work [1]. The scheme is enhanced to make it multi-level identity based cryptography which proved to be more robust and provided high level of system security. The proposed scheme was applied to multicast group key management in WSN where it not only ensured highly secure communications in WSN but also showed significant improvement in terms of packet delivery ratio, CPU utilization, routing overhead and delay performance.

The remainder of the paper is structured as follows. This is the first section of the paper. Section II reviews relevant literature and provides useful insights from which actually the present work is motivated. Section III provides details of the proposed multi-level identity based encryption scheme. Section IV presents simulations and results. Section V concludes paper and gives directions for future work.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

2. PRELIMINARIES

This section provides basics of IBC. However, a review of IBCs predecessors such as private key cryptography, public key cryptography and PKI can be found in our prior work [1]. IBC has two important mechanisms namely ID-Based Encryption (IBE) and ID-Based Signature (IBS). The IBE involves setup, extraction of private key, encryption and decryption while the IBS involves setup, extraction of private key, signature and verification. The setup and private key extraction phases of IBE and IBS are identical. Further discussions on the basics of IBC and our proposed multi-level identity based cryptography are based on the scenario illustrated in Figure 1. The parties involved in this scenario are used repeatedly in this paper.

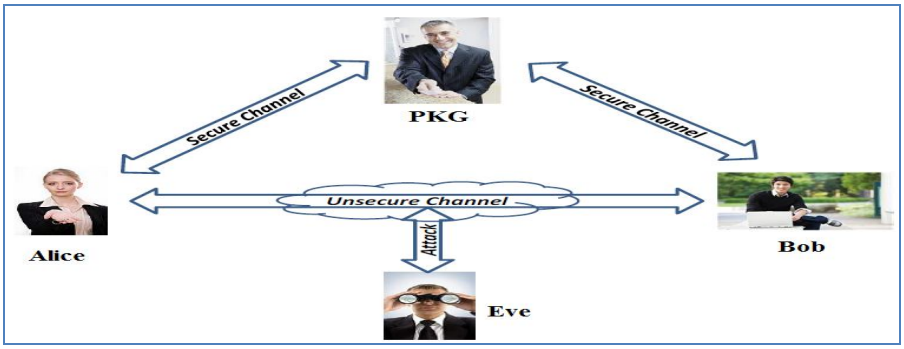

Figure 1 – Parties involved in communication

There is secure communication channel between Private Key Generator (PKG) and User1 and PKG and User2. The communication channel between User1 and User2 is insecure where there is ever possibility to have an adversary to launch attacks. The PKG is the trusted third party that provides security keys as required by IBC.

2.1 Setup and Private Key Extraction Phases of IBE and IBS

In the setup phase, PNG chooses a secrete value ***s*** randomly. The value of ***s*** remains secret as PNG keeps it for itself. Additionally, the PNG generates a public key for itself and makes it available to all other parties such as User1 and User2. In the private key extraction phase PNG generates private keys for all the parties such as User1 and User2. User1 and User2 can obtain their private respective private keys via secure channel.

2.2 Encryption and Decryption Phases of IBE

With respect to the scenario illustrated in Figure 1, User2 wants to send a message to User1 and ensure that the message reaches User1 securely. First of all User2 takes publicly known ID of User1 and applies function F in order to obtain public key of User1. Then User2 encrypts message using public key of User1 and sends it to User1. User1 receives that message and decrypts it using her own private key.

2.3 Signature and Verification Phases of IBS

Before sending a message to User1, User2 signs the message by using his own private key. Then the message along with signature is sent to User1. This is the process involved in the signature phase. In the verification phase, User1 takes message sent by User2. Then User1 applies function F to the publicly known ID of User2 in order to obtain his public key. Once public key is known, User1 can verify the signature of User2 by using User2's public key thus authenticating the party from which message has been received.

2.4 Enhanced Identity Based Cryptography

This is our extension to the EIBC scheme proposed in [1]. It has assumptions similar to that of Nicanfar and Leung [4]. It makes use of Pseudo Random Number Generator (PRNG) and Periodic Modification Functions (PMFs). Setup, Encryption, Decryption algorithms of EIBC are as follows.

2.4.1 *SETUP Algorithm*

Algorithm: Setup in EIBC

01 PKG selects secret values to compute its own public key
02 PKG takes three hash functions
03 PKG forms system parameters used for security primitives
04 User A and B get public key of PKG
05 Both A and B can have mutual access their public keys
06 PKG extracts private key of B and sends it to B
07 B also can compute its private key using parameters known
08 B can verify the private key of his own

This algorithm is used to have security primitives at the time of setup. The security primitives are used in further interactions in WSN.

2.4.2 Encryption Algorithm
Algorithm: Encryption in EIBC (Encrypted communication between sender (A) and receiver (B)

01 A uses B's ID and computes public key of B
02 A users random variables and generate U and V values
03 A sends C=(U,V) to B after encryption

This algorithm is meant for achieving ID based encryption. It will ensure encrypted communication between two parties in the network.

2.4.3 Decryption Algorithm
Algorithm: Decryption in EIBC (between sender (A) and receiver (B)

01 B receives encrypted message from A
02 B uses its own private key
03 B decrypts the message

This algorithm is meant for achieving decryption. It will ensure encrypted communication between two parties in the network and participates in the decryption process.

3. MULTI-LEVEL IDENTITY BASED CRYPTOGRAPHY

This section presents our proposed multi-level identity based key exchange scheme that can be used along with cryptography to secure WSN. As illustrated in Figure 1, two parties namely User1 (A) and User2 (B) involve in secure communications using this scheme. Both parties have multi-level identities that are used to ensure security. The scheme is based on three algorithms namely Setup, Extract and Key Agreement. The secure communication mechanism is as shown in Figure 2. There are three parties involved in the communication process.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

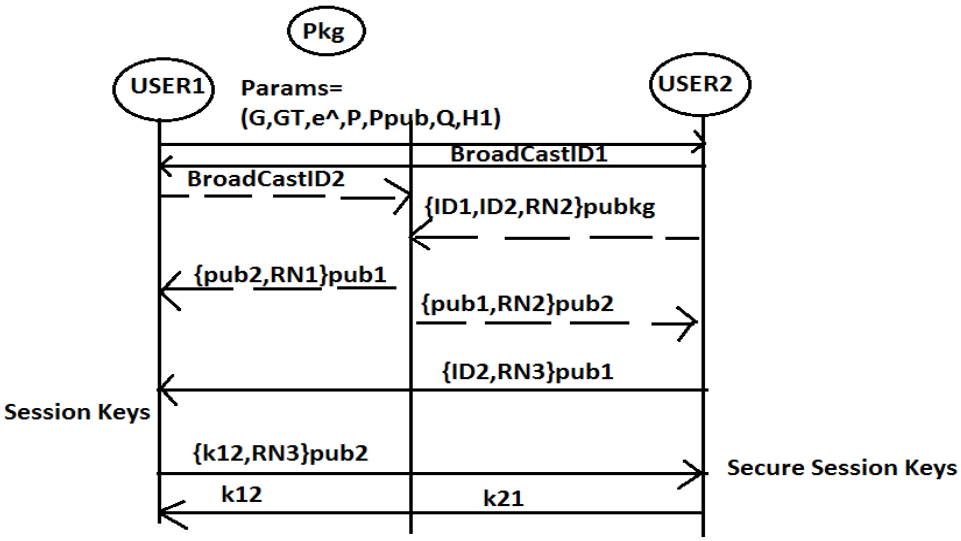

Figure 2 – Secure communication scenario

As shown in Figure 2, it is evident that PKG is involved in private key generation while the other parties such as User1 and User2 will have security communications. The three algorithms involved in the process are setup, extract and key agreement.

3.1 Setup

This algorithm is meant for setting up an environment where secure communications is possible. It takes a security parameter and generates system parameters that can be used in other phases such as Extract and Key Agreement.

Algorithm: Setup
Inputs: Security parameter l
Output: System secret keys, parameter list

1 PKG takes l as input
2 PKG chooses a cyclic additive group G using P
3 PKG chooses a cyclic multiplicative group GT
4 PKG chooses a prime order q
5 A bilinear map exists as $\hat{e}$:G× $G \rightarrow G_T$
6 PKG chooses a master secret $s \epsilon Z_q^*$
7 PKG sets $P_{pub=} s^P$
8 PKG randomly chooses $Q \epsilon G$
9 PKG chooses cryptographic hash function $H_{1:\{0,1\}} * \rightarrow G$
10 The final system parameter list $params = (G, G_T, \hat{e}, P, P_{pub,Q,H_1})$

Figure 3 – Algorithm for Setup

As shown in Figure 3, the setup in the proposed scheme finally produces system parameters that are useful in further communications in WSN. The parameters include cyclic additive group, cyclic multiplicative group, bilinear map, cryptographic hash function, and so on. Figure 3 shows primary key extraction process that is given by PKG.

3.2 Extract

This subsection provides the procedure for extracting primary key as part of the proposed multi-level identity based cryptography. Here master secret and multi-level identities are given as input while the procedure returns private key.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

Algorithm: Extract
Inputs: User's multi-level identities, master secret s
Output: private key
1 *Compute* $P_{i,u=H_1(ID_{i,u})}$ where $1 \leq u \leq n$
2 *Choose a random* $r_{i,u} \in Z_q^*$ and computes $R'_{i,u}=r_{i,u}P$.
3 *Compute* $S'_{i,u}= r_{i,u}Q+sP_{i,u}$.
4 *Compute* $S_{i=\sum_{u=1}^{n} S'_{i,u}}$ and $R_{i=\sum_{u=1}^{n} R'_{i,u}}$
5 *Send the private key* $d_{i=}(S_i, R_i)$ to user through secure channel

Figure 4 – Illustrates extraction process

The private key extraction is required by all parties involved in secure communications. For instance, both User1 and User2 need such key in order to participate in usage of security primitives as part of multi-level identity based cryptography. The private key generated by PKG and sent to users through secure channel.

3.3 Key Agreement

In the proposed scheme, this is the crucial phase in which secure shared session is established between two communicating parties. The parameters of the two parties are used and a common shared session key is established.

Algorithm: Key Agreement
Inputs: Parameters of two participant nodes A and B
Output: A common shared session key
1 A chooses a random value $x \in Z_q^*$
2 A computes $T_{A,1=xP}$, $T_{A,2=-xQ^B}$
3 A computes $T_{A,3=x\sum_{j=k+1}^{n} P_{B,j}}$
4 A sends to B $T_{A=}(T_{A,1}, T_{A,2}, T_{A,3})$ to user B
5 B chooses a random value $y \in Z_q^*$
6 B computes $T_{B,1} = yP$, $T_{B,2} = -yQ^A$ and $T_{B,3} = y\sum_{j=k+1}^{m} P_{A,j}$
7 B sends to user A $T_B = (T_{B,1}, T_{B,2}, T_{B,3})$ to user A
8 A computes session secret keys $K_{AB,1} = e^{\wedge}(S_A, T_{B,1}) \cdot e^{\wedge}(T_{B,2}, R_A) \cdot e^{\wedge}(T_{B,3}, -P_{pub}{}^A) \cdot e^{\wedge}\left(\sum_{j=1} P_{B,j,P_{pub}^B}\right) x$.

$$K_{AB,2} = x \cdot T_{B,1=}xyP$$

8 B computes session secret key

$K_{BA,1=} e^{\wedge}(S_B, T_{A,1}) \cdot e^{\wedge}(T_{A,2}, R_B) \cdot e^{\wedge}\left(T_{A,3}, -P_{pub}B\right) \cdot e^{\wedge}\left(\sum_{j=1}^{k} P_{A,j,P_{pub}^A}\right) y$

$$K_{BA,2} = y \cdot T_{A,1=}xyP$$

9 Secure session established

Figure 5 – Illustrates key agreement

As shown in Figure 4, it is evident that the key agreement phase involves two communicating parties. User2 takes private key from PKG. User2 signs a message and encrypts it and sends it to User1. User1 applies F to multi-level identity of User2 and gets public key of User2. The encrypted message is decrypted by User1 using her private key. After decrypting the message, User1 verifies the signature received from User2 using User2's public key. The correctness of the proposed scheme can be verified as described in the ensuing sub section.

3.4 Correctness Verification

By taking user A as an example, this subsection provides correctness proof of the proposed scheme. Both users involved in the communication can compute session keys. When both session keys are identical, it is said to have secure session between two nodes or users.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

$$sK_{AB,1} = e^{\wedge}\left(S_{A,}T_{B,1}\right).\ e^{\wedge}\left(T_{B,2,}R_{A}\right).\ e^{\wedge}\left(T_{B,3,-}P_{pub}{}^{A}\right).\ e\wedge\left(\sum_{j=1}P_{B,j,}P_{pub}^{B}\right)x\ .$$

$$= e^{\wedge}\left(\sum_{j=1}^{m}S^{AP_{A,j,}y^{P}}\right).e\wedge\left(\sum_{j=1}^{m}r_{A,j}Q^{A},y^{P}\right).\ e^{\wedge}\left(-yQ^{A.}\sum_{j=1}^{m}r_{A,j}P\right).e^{\wedge}\left(y\sum_{j=k+1,-}^{m}s^{A}P\right).e^{\wedge}\left(\sum_{j=1}^{k'}P_{B,j,}P_{pub}^{B}\right)x$$

$$= e\wedge\left(\sum_{j=1}^{k}s^{AP_{A,j,}y^{P}}\right).e^{\wedge}\left(\sum_{j=k+1}^{m}sAP_{A,j,y^{P}}\right).e^{\wedge}\left(y\sum_{j=k+1}^{m}P_{A,j,-}{}^{s^{A}P}\right).e^{\wedge}\left(\sum_{j=1}^{k'}P_{B,j,}s^{BP}\right)x$$

$$= e^{\wedge}\left(\sum_{j=1}^{k}P_{A,j,}s^{AP}\right)y.e^{\wedge}\left(\sum_{j=1}^{k'}P_{B,j}P_{pub}{}^{B}\right)x$$

$$= e^{\wedge}\left(\sum_{j=1}^{k}P_{A,j,}P_{pub}{}^{A}\right)y.\ e^{\wedge}\left(\sum_{j=1}^{k}P_{B,j,}P_{pub}{}^{B}\right)x$$

In the same fashion B computes session key as follows.

$$K_{BA,1}= e\wedge\left(S_{B},T_{A,1}\right).e\wedge\left(T_{A,2},R_{B}\right).e\wedge\left(T_{A,3,-}P_{pub}B\right).\ e\wedge\left(\sum_{j=1}^{k}P_{A,j,}P_{pub}^{A}\right)y$$

$$= e^{\wedge}\left(\sum_{j=1}^{k}P_{A,j,}P_{pub}{}^{A}\right)y.\ e^{\wedge}\left(\sum_{j=1}^{k}P_{B,j,}P_{pub}{}^{B}\right)x$$

As shown in the above equations, the proposed approach could establish secure communication between two parties. Our extensive simulations reveal the utility of our proposed scheme. The ensuing section provides the results of our experiments.

4. SUMULATIONS AND RESULTS

In the presence of multi level identity based cryptography, we performed simulations of the proposed system. Simulations are made with NS2. Identity based cryptography has been enhanced in our previous work [1] while this paper focused on the multi-level identity based cryptography which renders more flexible and secure communications in WSN. The simulation environment is provided in Table 1 followed by simulation results.

Table 1: Shows simulation environment

PARAMETER	SPECIFICATION
Simulation tools used	NS2 Network Simulator (ns-2.35)
Simulation time	10 sec, 20 sec, 30 sec
Number of nodes	50, 100, 200, 300...
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	CBR [constant bit rate] [20]
Packet size	512bytes
Node mobility model	10 packets/sec
Protocol	AODV

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

As can be seen in Table 1, the simulation environment is described. The observations made in the presence of multi-level identity based cryptography include are presented below in terms of security analysis, packet delivery ratio, delay analysis and routing overhead.

Table 2 – Results of average delay

MIN SPACE IN N/W	EIBC	EIBCGKM	MIBC
0	65	55	45
2	70	61	50
4	89	73	60
6	114	96	80
8	130	115	100
10	165	139	125

As shown in Table 2, the average delay time for different schemes is presented.

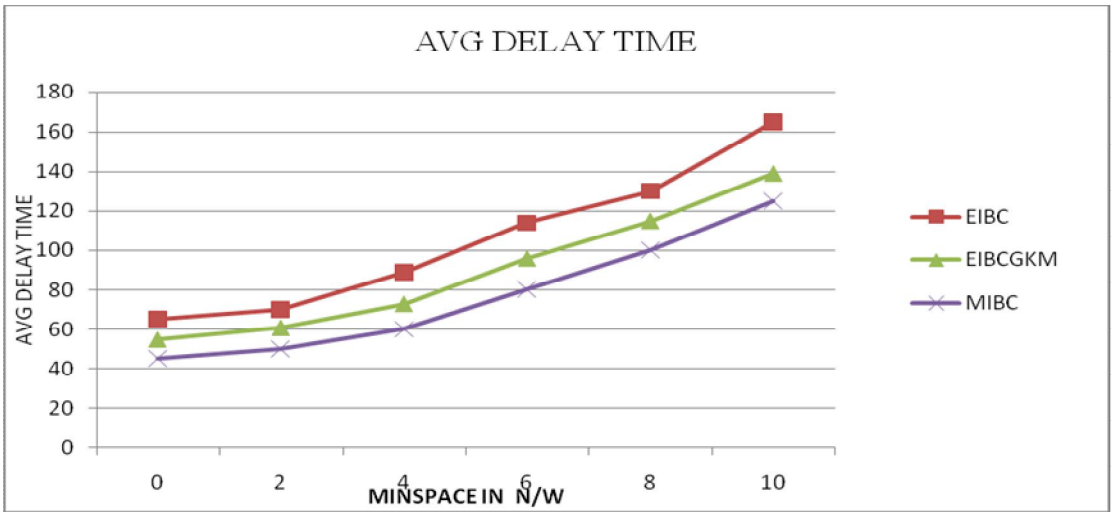

Figure 6 – Shows delay analysis

As shown in Figure 5, it is evident that the horizontal axis represents load time while the vertical axis represents delay time. From the results it is understood that as load time increases, the delay decreases. However, there is significance improvement in the proposed approach MIBC when compared with the existing one.

Table 3 – Shows packet delivery ratio

Packet rate	EIBC	EIBCGKM	MIBC
0	12	19.6	25
1	14.5	25.2	30
1.8	23	32	45
2.4	30	38	50
2.8	35	42	55
3.3	38	48	57
3.6	46	52	59
4.2	55.6	65	75
4.8	59	67	78

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016 ISSN 2321-5992

As shown in Table 3, the percentage of data packets delivered with given packet rate.

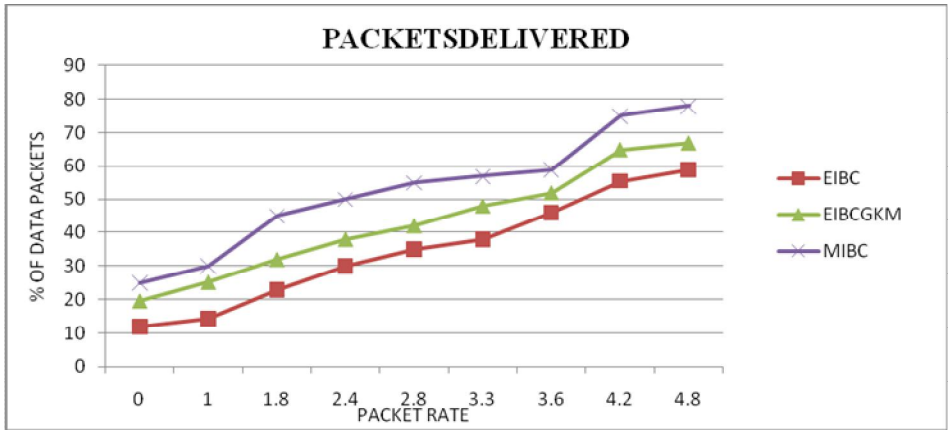

Figure 7 – Shows comparison of packet delivery ratio

As shown in Figure 7, it is evident that the horizontal axis represents simulation time while the vertical axis represents number of packets. From the results it is understood that as simulation time increases, the packet delivery ratio increases. However, there is significance improvement in the packet delivery ratio of the proposed approach when compared with the existing one.

Table 4 – Shows computational cost

MIN SPACE IN N/W	EIBC	EIBCGKM	MIBC
0	1330	1700	1050
2	910	1090	370
4	580	890	240
6	465	780	170
8	390	660	190
10	390	580	150

As shown in Table 4, the computational cost of different schemes is presented.

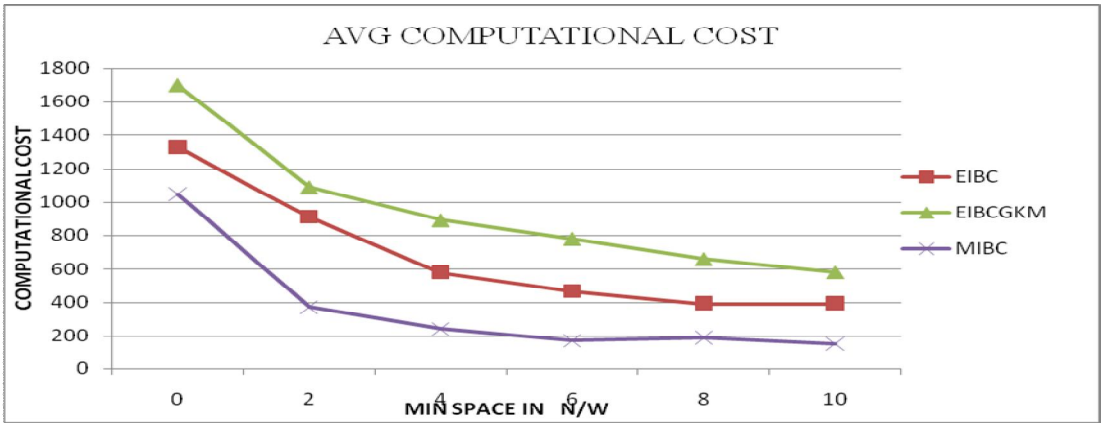

Figure 8 – Average computational cost

As shown in Figure 8, it is evident that the computational cost of the proposed system is low when compared with other schemes. As the simulation time is going on the computational cost is reduced.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation .....
Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016
ISSN 2321-5992

Table 5 – Shows results of computational cost in the presence of link failure

LINK FAILURE	EIBC	EIBCGKM	MIBC
0	205	280	180
4	205	290	175
8	200	330	160
12	225	345	200
16	235	380	210
20	270	365	230

As shown in Table 5, the computational cost in the presence of link failure is presented for different schemes.

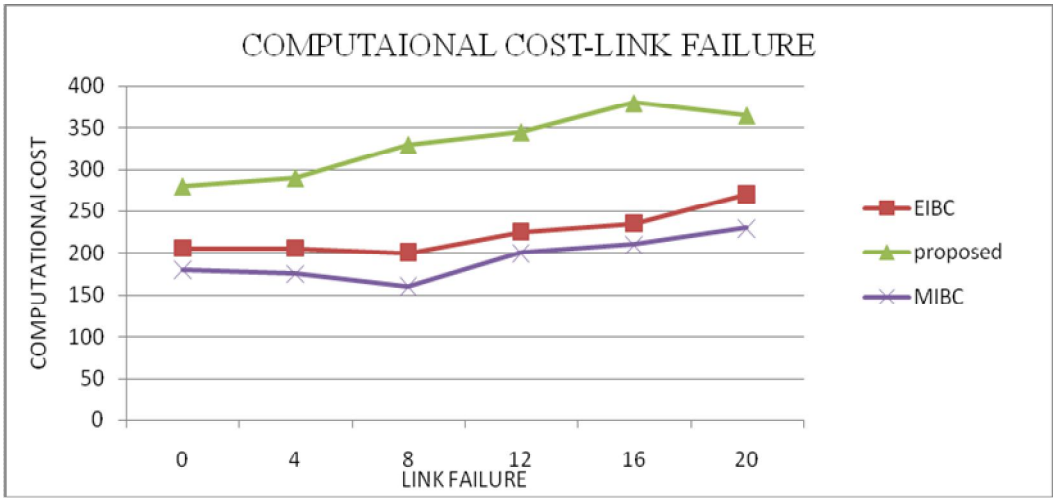

Figure 9 – Computational cost vs. link failure

As shown in Figure 9, the computational cost in the presence of link failure is presented. The proposed system namely MIBC is found to perform when as it shows least computational cost. Link failure is represented in horizontal axis while the vertical axis represents computational cost.

Table 6 – Impact on delivery links

MIN SPACE IN N/W	EIBC	EIBCGKM	MIBC
0	170	250	300
1	175	260	295
1.8	180	265	290
2.4	185	270	295
2.8	190	275	298
3.3	195	280	299

As shown in Table 6, the impact of delivery links in terms of delivery ration is presented for different schemes.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation .....
Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016
ISSN 2321-5992

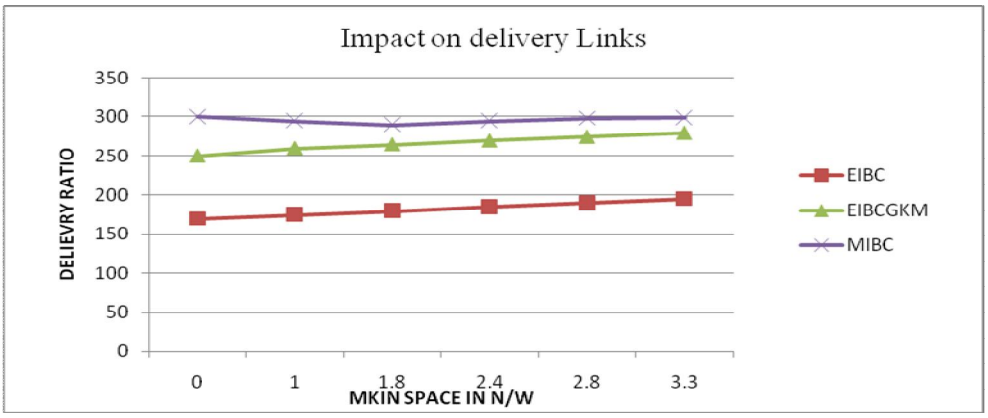

Figure 10 – Impact on delivery links

As shown in Figure 10, the delivery ratio is presented in the context of impact on delivery links. The results are plotted for three different schemes. However, the proposed scheme MIBC shows higher performance when compared with other ones.

Table 7 – Communication overhead

Time	EBIC	EIBCGKM	MIBC
0	55	65	45
1	45	55	40
1.8	40	48	30
2.4	41	49	29
2.8	43	51	34
3.3	30	52	25
3.6	34	45	26
4.2	25	35	20

As shown in Table 7, the communication overhead is presented for different schemes.

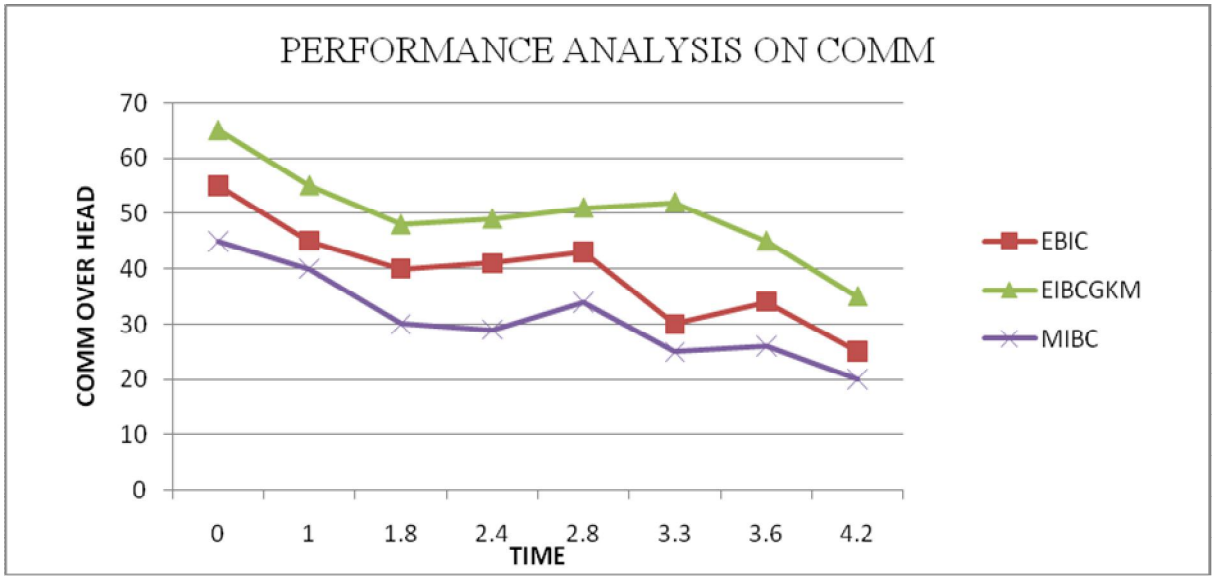

Figure 11 – Communication overhead

As shown in Figure 11, it is evident that the performance of different schemes is compared in terms of communication overhead. The communication overhead of the proposed scheme MIBC appeared to be less when compared with other ones.

5. DISCUSSION

Recent research carried out by Recently Nicanfar and Leung [4] proposed Enhanced Identify Based Cryptography (EIBC) for efficient key management. In our previous paper we proposed a mathematical model for enhanced identity based cryptography towards multicast group key management which can be used in various real world applications. Our simulation results in the previous paper [1] revealed that the proposed scheme is highly secure and its performance is significantly improved in terms of delay performance (Figure 6 of [1]), PDR (Figure 8 of [1]), average computational cost (Figure 7 of [1]), and impact on delivery links (Figure 9 of [1]), computational cost-link failure (Figure 10 of [1]) and communication overhead (Figure 11 of [1]). In this paper we proposed a multi-level identity based cryptography scheme that could be applied to multicast group key management. Precisely, the multi-level identity based cryptography proposed by us can be used for secure digital authentication which brings about high level of system security. We proposed Multi-level Identity Based Cryptography (MIBC) for the first time and explored its utility in maximizing security in WSN. The scheme proposed by us in [1] is enhanced to make it multi-level identity based cryptography which proved to be more robust and provided high level of system security.

The proposed scheme in this paper provides not only highly secure communications in WSN but also showed significant improvement in terms of packet delivery ratio, average delay time, average computational cost, computational cost-link failure, impact on delivery links, and communication overhead. The performance improvement in terms of delay is shown in Figure 6, packet delivery ratio in Figure 7, average computational cost in Figure 8, computational cost vs. link failure in Figure 9, impact on delivery links in Figure 10, and communication overhead in Figure 11. Our scheme when compared with [4] and [1] shows significant improvement in terms of aforementioned parameters.

6. CONCLUSIONS AND FUTURE WORK

In this paper we studied multi-level identity based cryptography in WSN. This is an extension to our enhanced identity based cryptography for efficient group key management in WSN [1]. Ever since Shamir introduced IBC in 1984, it has been providing promising solutions for complete, light weight and secure communications in WSN. It could overcome the limitations of traditional PKI infrastructure such as complexity and overhead. The rationale behind this is that, IBC could make eliminate costly third party certificates and verification process besides making key management simple. With IBC it is possible to use any publicly known identity to generate security keys so as to make it intuitive and can be used by people without technical knowhow of cryptography. In this paper we proposed a multi-level identity based cryptography scheme that could be applied to multicast group key management. Since multi-level identity is flexible and renders scalable and secure communications, it can be used in real time applications where nodes can have identities at different levels which resemble real world transactions. Precisely, the multi-level identity based cryptography proposed by us can be used for secure digital authentication which brings about high level of system security. Our extensive simulations reveal that the proposed scheme is flexible, scalable and provide high level of security to communications in WSN. Applying our scheme to other wireless networks such as MANET, VANET and analysing how it works is an important direction for future work.

REFERENCES

[1]. Sumalatha and Satyanarayana (2015). Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN. International Journal of Application or Innovation in Engineering & Management, p1-13.
[2]. A. Shamir, ”Identity-based Cryptosystems and Signature Schemes,” Advances in Cryptology - CRYPTO, LNCS 196, pages 47-53, Springer-Verlag, 1984.
[3]. D. Boneh and M. Franklin, ”Identity-Based Encryption from the Weil Pairing,” Advances in Cryptology - CRYPTO, LNCS 2139, pages 213-229, Springer-Verlag, 2001.
[4]. Nicanfar, H., Leung, V. C. M. (2012). EIBC: Enhanced Identity-Based Cryptogrphy, a Conceptual Design. IEEE, p1-7.
[5]. Sumalatha and Satyanarayana (2014). A Review on Multi-Level Identity Based Cryptography for Secure Digital Signature Authentication. International Journal of Computer Engineering and Applications, p1-12.
[6]. J. Baek, J. Newmarch, R. Safavi-Naini and W. Susilo, ”A Survey of Identity-Based Cryptography,” in Proc. of Australian Unix Users Group Annual Conference, pages 95-102, Australia, 2004.
[7]. C. Gentry and A. Silverberg, ”Hierarchical ID-Based Cryptography,” ASIACRYPT, LNCS 2501, pages 548-566, Springer-Verlag, 2002.
[8]. H. W. Lim and K. G. Paterson, ”Identity-Based Cryptography for Grid Security,” in Proc. of the First International Conference on e-Science and Grid Computing, Melbourne, Australia, Dec. 2005.
[9]. A. Menezes, ”An Introduction to Pairing-Based Cryptography,” Notes from lectures given in University of Waterloo, 2005.

[10]. H. Nicanfar, P. Jokar and V. C.M. Leung, "Smart Grid Authentication and Key Management for Unicast and Multicast Communications," in Proc. IEEE PES ISGT Conference, Perth, Australia, Nov. 2011.
[11]. H. Nicanfar, P. Jokar and V. C.M. Leung, "Efficient Authentication and Key Management for the Home Area Network," to be presented at IEEE ICC Conference, Ottawa, ON, June 2012.

AUTHOR.

Prof. B.Sathyanarayana received his B.Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985, Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri Krishnadevaraya University, Anantapuramu, A.P. India. He has 24 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals

P.Sumalatha received her M.Sc in Computer Science and Technology from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007. She is currently pursuing her Ph.D in Computer Science and Technology at Sri Krishnadevaraya University, Anantapuramu, A.P., India. Her current research interest includes Computer Networks