Secure and efficient data transmission in wireless sensor networks using elliptical curve cryptography

Varsha .S. Chare

Department of computer science and engineering,
PDA college, Gulbarga,
585101, India

Dr. Jayashree.Patil

Department of computer science and engineering, PDA college, Gulbarga
585101, India

***Abstract*- Data forwarding in WSN is insecure as wireless protocol provides least security measures. Hence in this work we propose a security extension with the help of two techniques: Passive SET-IBS (Secure and efficient transmission in identity based signature) and active SET-IBOOS (Secure and efficient transmission in identity based online offline signature) technique using Diffie Hellman elliptical curve cryptography. In this work we have developed a sensor network model in Mat lab to incorporate Physical-Mac layer fundamentals of modulation, channel error, transmission delay and bit error rate into the simulation to realistically analyze the behavior of this network and concept. Further simulation results have been demonstrated to show the effectiveness of proposed work in terms of minimization of energy consumption, reducing bit error rate and also delay.**

Keywords: *SET-IBS, SET-IBOOS, cluster head, elliptical curve cryptography.*

1. INTRODUCTION

WSN is a multi hop wireless network that consists of low cost low power sensor nodes which are capable of sensing, computation and communication.WSN take advantage of deployment rapidly and strong survivability without fixed network support but also with features of dynamic topology structure and energy resources are limited and so on. The application of WSN technology is a revolution of perceived and collection of information and used for various applications[1].Routing in WSN is very challenging due to the inherent characteristics that distinguish this networks from other wireless networks like mobile ad hoc networks or cellular networks. Sensor nodes are tightly constrained in terms of energy, processing and storage capacity. They require careful resource management. Energy efficient routing method is proposed for WSN which consists of large number of energy constrained sensors and a few hubs as the CH of sensors. Since each battery powered sensor only has limited energy resource and the battery recharge or replacement is impractical. A network with energy aware design becomes important to achieve the desired performance. Energy is one of the scarcest resource of WSN nodes and it determines the lifetime of WSN's. WSN's are deployed in large numbers in various environments including remote and hostile regions. Along with minimization of energy providing security to data is also important because sensor network is in secured as wireless protocol provides least security measures. Hence in this paper two protocols are proposed that provide security extension.

SET-IBS and

SET-IBOOS based on diffie-hellman elliptical curve

cryptography

ISSN: 2278 – 1323

2. RELATED WORKS

This section covers literature survey of the work of this paper

In [1], a survey of security issues in wireless sensor networks WSN's is done. As WSN suffers from many constraints like low computation capability, small memory, limited energy resources and use of insecure wireless communication channel.There are 5 security issues : Cryptography, key management, secure routing, secure data aggregation and intrusion detection

In [2], survey of various algorithms is done. These algorithms can help in overcome some of the WSN challenges specified in [1]. Comparison between different clustering algorithms is done. Author presented a taxonomy and general classification of published clustering schemes and different clustering algorithms for WSNs

In [3], author develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro sensor networks that combines the ideas of energy-efficient cluster-based routing as specified in [2] and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH

In [4], the advances in technology have made it possible to have extremely small, low powered sensor devices equipped with programmable computing, multiple parameter sensing, and wireless communication capability. But, because of their inherent limitations, the protocols designed for such sensor networks must efficiently use both limited bandwidth and battery energy. Author developed an M/G/1 model to analytically determine the delay incurred in handling various types of queries using enhanced **APTEEN** (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) protocol.

In [5], author proposes PEACH protocol, which is a power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks. By using overhearing characteristics of wireless communication, PEACH forms clusters without additional overhead and supports adaptive multi-level clustering. In addition, PEACH can be used for both location-unaware and location-aware wireless sensor networks. But implementation is complicated

In [6], some of implementation problems in [5] are addressed. Sensors used for these purposes needs to be deployed very densely and in a random fashion. They should be able to operate without human intervention. Clustering is a technique employed to increase the various capabilities of a sensor network. Design and implementation issues of clustering algorithms employed in sensor networks, formation of cluster of nodes with a CH for each cluster are discussed.

In [7], Cluster-based communication has been addressed for these networks for various reasons such as scalability and energy efficiency. The problem of adding security to cluster based communication protocols for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources, and propose asecurity solution for LEACH,a protocol where clusters are formed dynamically and periodically. Solution uses building blocks from SPINS

In [8], symmetric key management technology for security uses more amount of energy and computation overhead is also more. Author introduced the different parameters to measure the performance of clustering protocols, namely, energy dissipated, delay and quality of aggregated data.

Based on the literature surveyed above, security issues of WSN and minimization of energy consumption during data transfer are considered as serious issues

3. SYSTEM DESIGN

In this section, the emphasis is given on the explanation of architecture of design and the proposed solution of the work is defined

ISSN: 2278 – 1323

A. Proposed solution

The main aim of the proposed work is to provide security for the data in wireless network as the data is to be passed through wireless channel. Therefore, two security protocols SET-IBS and SET-IBOOS are proposed. With the help of these two protocols energy consumption can also be reduced as shown in the simulation results.

B. System Architecture

Workflow of SET-IBS Protocol and its Operation

Secure communication in SET-IBS relies on ID based cryptography in which user public keys are their ID information. Thus, users can obtain their corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy. Fig 5 illustrates the process of encryption and decryption using the keys generated. As shown in fig private key is generated from nodes ID and the mask (msk) function of Base station (BS). Similarly, public key is generated from msk function of CH. Using these keys security can be provided to the data.

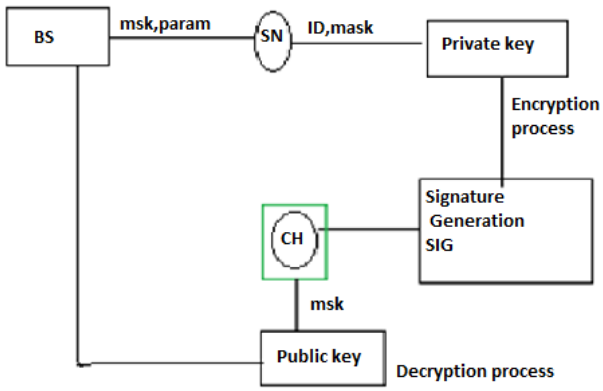


Fig 1: Workflow of SET-IBS protocol

Workflow of SET-IBOOS and its Operation

SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem.Private key is generated in similar way as that of IBS, Along with private key online signature is generated for encrypting the data. This online signature is obtained using offline signature. While decrypting the data online signature, sensor node ID and message M parameters are used as shown in fig 2

ISSN: 2278 – 1323

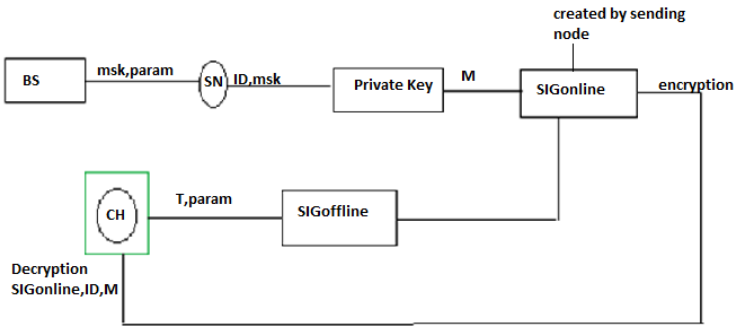


Fig 2: Workflow of IBOOS protocol

4. Simulation Results

In this work we have developed a sensor network model in Matlab to incorporate Phy-Mac layer fundamentals of modulation, channel error, transmission delay and bit error rate into the simulation to realistically analyse the behaviour of this network and concept. We compare the performance of both the techniques(IBS and IBOOS) for various parameters as shown in the graph.

A. Simulation Parameters

Table 1. Simulation parameters

	Values
Network area	100 m x100 m
Number of nodes	40
Message size	50 bits
Signal-to-noise ratio(SNR)	-40 db
Initial energy of nodes	0.5 Joules
MAC layer	IEEE 802.11
Base station location	10-50m

B. Simulation performance metrics

The performance metrics used to measure the simulation of the work are explained below

- Energy consumption:

  Energy consumption in the WSN cluster head is given by

  equation 1 below

ISSN: 2278 – 1323

$$E_{bs}(k_c) = -\frac{1}{\pi k_c}(1+\alpha)N_f\sigma^2\ln(P_b)G_1M^2M_l + \frac{P_{ct}+P_{cr}}{B} \quad (1)$$

Where,

kc is the number of clusters

α is the efficiency of radio frequency (RF) power amplifier

Nf is the receiver noise figure

σ2=No/2 is the power density of additive white Gaussian noise (AWGN) channel

Pb is the bit error rate (BER) obtained while using phase shift keying

G1 is the gain factor

M1 is the gain margin

B is the bandwidth

Pct is the circuit power consumption of the transmitter

Pcr is the circuit power consumption of the receiver.

- Bit error rate:

Bit errors is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors.

$$\text{BER} = \frac{\text{number of bit errors}}{\text{Total number of transferred bits during a time interval}}$$

- Signal to noise ratio (SNR):

The ratio of the strength of electrical or other signal carrying information to that of unwanted interference

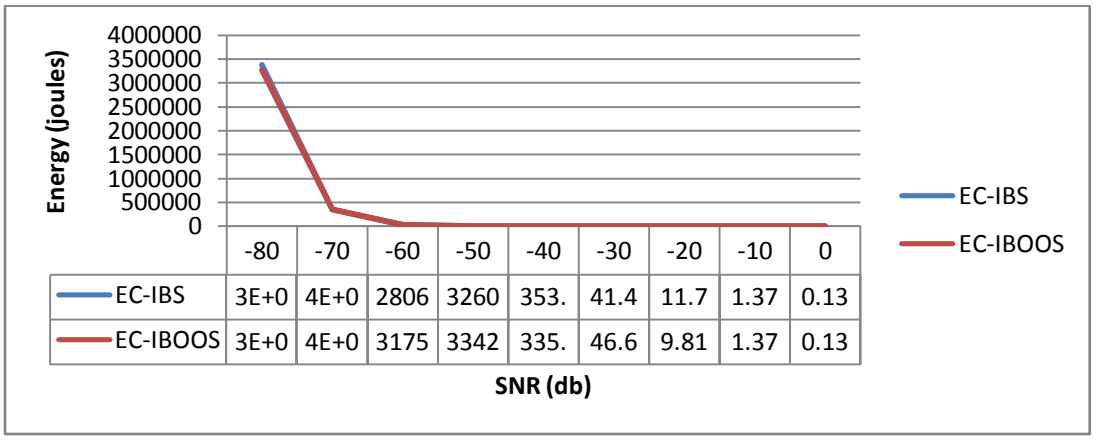
ISSN: 2278 – 1323

➢ Delay:

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds.

C. Simulation Results

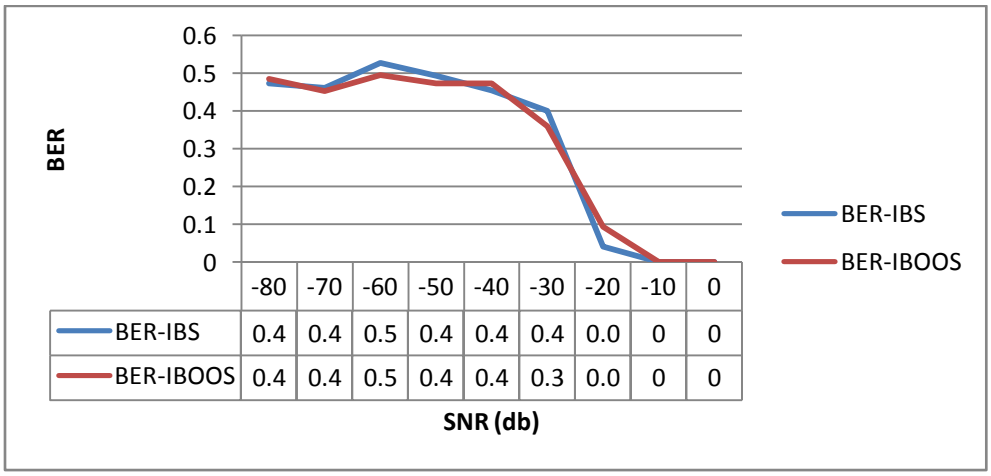
In this section, the graphical analysis of the work is done depending on the values obtained from the simulation environment. These graphs are plotted on the performance metrics described earlier.



	-80	-70	-60	-50	-40	-30	-20	-10	0
EC-IBS	3E+0	4E+0	2806	3260	353.	41.4	11.7	1.37	0.13
EC-IBOOS	3E+0	4E+0	3175	3342	335.	46.6	9.81	1.37	0.13

Fig 3 graphs showing the comparison of energy consumption of SET- IBS and SET-IBOOS

Figure 3 illustrates how the energy value reaches to zero when the strength of the signal is stronger compared to that of noise.Here in both IBS and IBOOS technique energy consumption value has reached to zero as SNR value is zero. This is one of the strongest parameter that helps in efficient transmission of data by minimizing energy consumption.



	-80	-70	-60	-50	-40	-30	-20	-10	0
BER-IBS	0.4	0.4	0.5	0.4	0.4	0.4	0.0	0	0
BER-IBOOS	0.4	0.4	0.5	0.4	0.4	0.3	0.0	0	0

Fig 4 comparison of BER of SET-IBS and SET-IBOOS

ISSN: 2278 – 1323

In figure 4 the bit error rate for both the IBS and IBOOS technique is shown. Here initially bit error rate for IBS technique is more compared to that of IBOOS but as the strength of the signal increases compared to that of noise then the value of bit error rate reaches to zero as shown above.

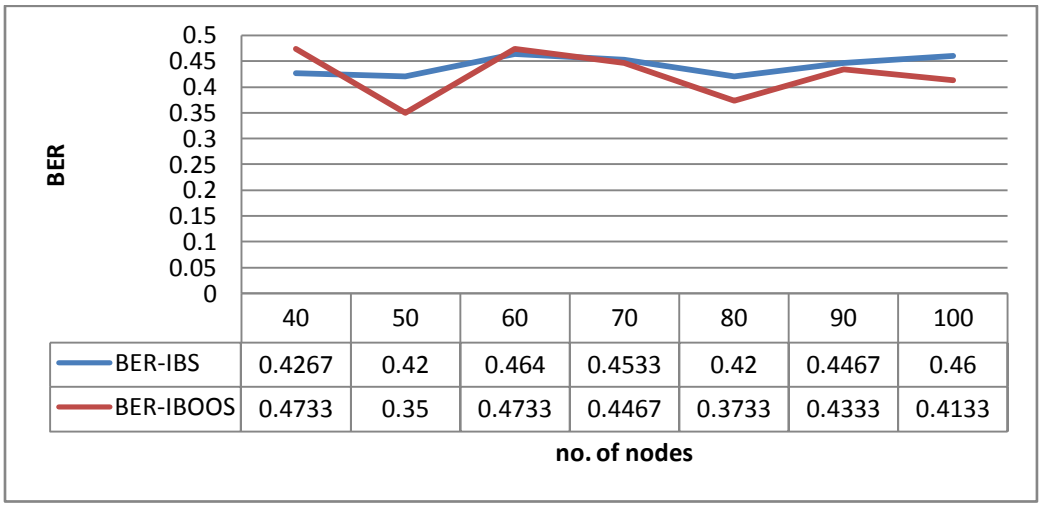


Fig 5 comparison of BER as number of nodes vary

The security provided by IBOOS technique is more as compared to that of IBS. So, figure 5 illustrates bit error rate in IBS is more compared to that of IBOOS.

5. Conclusion

Two secure and efficient data transmission protocols for CWSNs, SET-IBS and SET-IBOOS are implemented. In the evaluation section, feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks is provided. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly the comparison in calculation and simulation results show that even though both protocols are efficient but IBOOS is the more powerful protocol in providing security and also consumes less amount of energy as compared to that of IBS.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, *Stud. Comput. Intell.*Springer-Verlag, 2010, vol. 278.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, pp. 1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.

ISSN: 2278 – 1323

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, pp. 23–28, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc. IEEE NCA*, 2007, pp. 145–152.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in *Proc. WiCOM*, 2008, pp. 1–5.

[11]" A New Clustering Method to Prolong the Lifetime of WSN" Hamid Daneshvar Tarigh, Masood Sabaei

[12] S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," in *Proc. ICCCS*, 2011, pp. 146–151.

[13] G. Gaubatz, J. P. Kaps, E. Ozturk *et al.*, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in *Proc. IEEE PerCom Workshops*, 2005, pp. 146–150.

[14] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[15] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985, vol. 196, pp. 47–53.

[16] D. W. Carman, "New Directions in Sensor Network Key Management," *Int. J. Distrib. Sens. Netw.*, vol. 1, pp. 3–15, 2005.

[17] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Proc. IEEE CIT*, 2010, pp. 882–889.

[18] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

[19] J. Sun, C. Zhang, Y. Zhang *et al.*, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, 2010.

[20] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures,"in *Lect. Notes. Comput. Sc. - CRYPTO*, 1990, vol. 435, pp. 263–275.

ISSN: 2278 – 1323