Engineering and Scientific International Journal (ESIJ)
Volume 5, Issue 3, July – September 2018
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Security and Efficiency during Data Transmission in Wireless Sensor Networks

A.Arun kumar[#1], R.Anitha[*2]

[1]*Department of Computer Applications, SA Engineering College, Chennai, India*
Arun28496@gmail.com
[2]*Asst. Prof, Department of computer Applications,* SA Engineering college, Chennai, India

Abstract— Nowadays wireless sensor networks are mostly used for environmental control, surveillance tasks, monitoring, tracking and controlling etc. For this, the wireless sensor network has to be safe and efficient. Clustering is one of the most successful techniques to improve system performance in Wireless Sensor Network(WSN). Security is based on Digital Signature and which is using two protocols, Secure and Efficient data Transmission by Identity Based digital Signature (SET IBS) and Secure and Efficient data Transmission by Identity Based Online/Offline digital Signature (SET IBOOS). Most probably, the Elliptical Curve Cryptography (ECC) algorithm is used for data transmission. By using these protocols, the attacker can be recognized easily and energy burning is also reduced. In this paper, we maximize the time of first node dies (FND) in a WSN to extend the network lifetime.

Keywords *— Clustering; Secure and Efficient data Transmission by Identity Based digital Signature; Secure and Efficient data Transmission by Identity Based Online/Offline digital Signature; Elliptical Curve Cryptography; Energy consumption.*

1. Introduction

Wireless sensor network consists of small sized, light weighted, low power, low-cost wireless nodes called sensor nodes. It is measured by physical parameters such as sound, temperature, pressure, humidity and light. Sensor nodes have the capability to communicate either among each other or straight to a base station[1]. In a cluster-based WSN (CWSN), each cluster has a chief sensor node, known as cluster-head (CH) [2]. A CH collects the data gathered by the leaf nodes in its cluster, and send the data to the base station (BS). A sensor node of one cluster can only communicate with sensor node of other cluster by taking the authorization of the respective cluster. In this paper, we consider about secure data transmission with hierarchical clustering. In large-scale CWSNs, multi hop data transmission is used for transmission between CHs to the BS, Where the direct communication is not achievable due to the distance. A CH transmits data to the Base station by sending its data to its nearby nodes, in order the data are send to the BS. In SET-IBS and SET-IBOOS protocols the energy utilization is also reduce.

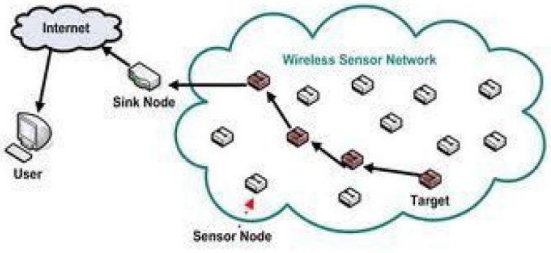

Fig.1: Wireless Sensor Network Architecture

2. Existing System

Nowadays, Energy Efficient Heterogeneous Clustered system for wireless sensor network is used for data transmission [3]. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol is an effective one to reduce and balance the total energy consumption for CWSNs. The Identity-Based Digital Signature (IBS) scheme, based on the trouble of factoring integers from Identity Based Cryptography (IBC), is to gain an entity public key from its identity information. The limitations or drawbacks of the existing system is adding security to LEACH-like protocol is complex, because they dynamically, randomly and periodically rearrange the network clusters and data links. SET-IBS and SET-DTA secure protocols for CWSNs, in terms of security overhead and energy consumption [4].

2.1 Disadvantages

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically reshuffle the network clusters [5] and data links. In this, energy consumption is superior to the SET-IBS and SET-IBOOS protocols. This minimizes the time of FND in a WSN and so it reduces the network duration.

3. Proposed System

For secure data transmission, the security is based on the Digital Signature. Here, Two protocols are used, SET IBS and SET IBOOS [6]. Secure communication in SET-IBS relies on ID based cryptography, in which user public

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

keys are having their ID information. SET-IBOOS is planned in order to reduce the computational overhead for security using IBOOS scheme. By using these protocols, the attackers can be recognized easily. Using this protocols, the energy consumption is also reduced [7]. In large-scale CWSNs, multi hop data transmission is used between the CHs and BS. The time of first node dies (FND), which indicates the length of sensor network is fully functional

3.1 Advantages

ECC uses short encryption key. This short key is faster and requires less computing power encryption algorithm. SET-IBS and SET-IBOOS use energy lower than the LEACH protocol. It minimizes the time of FND in a WSN and so it makes longer the network lifetime.

4. Methodology

4.1 SET IBS Protocol Operation

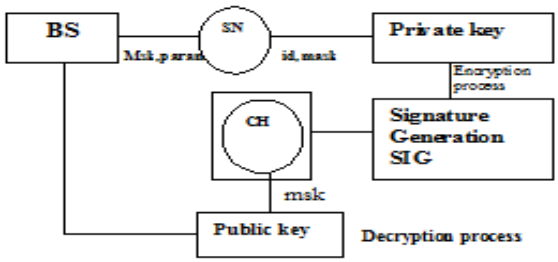

Fig.2: SET IBS protocol

Users can obtain their matching private keys without supplementary data transmission, which is efficient in communication and saves energy. This process illustrates the process of encryption and decryption using the keys generated. As shown in figure 2, private key is generated from nodes ID and the mask (msk) function of Base Station (BS). Likewise, public key is generated from msk of CH. By using these keys, the security can be provided to the data.

4.2 SET IBOOS Protocol Operation

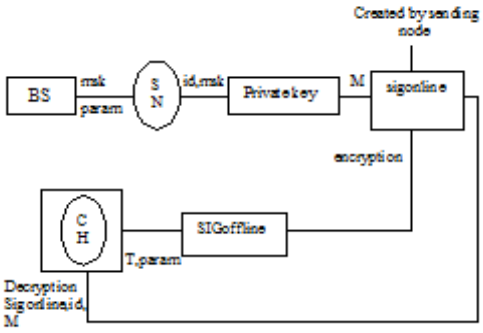

Fig 3: SET IBOOS protocol

SET-IBOOS is planned in order to reduce the computational overhead of security. Private Key is generated in a related way as that of IBS, online signature is generated for encrypting data. This online signature is obtained using offline signature, whereas for decrypting the data, online signature, sensor node ID and message M parameters are used as shown in fig 3. [8] The data encryption and decryption is done by using ECC. The ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over limited fields.

5. Implementation

Table 1 shows various parameters used for this work.

Table 1: Parameters

Parameters	Values
Network area	100m * 100m
Number of nodes	40
Message size	50 bits
Initial energy of nodes	0.5 joules
Base station location	10m-50m

4.2 Energy Consumption

In SET-IBS and SET-IBOOS protocol [9] the energy consumption in the WSN cluster head is specified by below equation,

$$E_{bs}(k_c) = -\frac{1}{\pi k_c}(1+\alpha)N_f\sigma^2\ln(P_b)G_1M^2M_1 + \frac{P_{ct}+P_{cr}}{B}$$

Where,

kc is the number of clusters

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

Nf is the receiver noise figure

σ2=No/2 is the power density of preservative 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

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

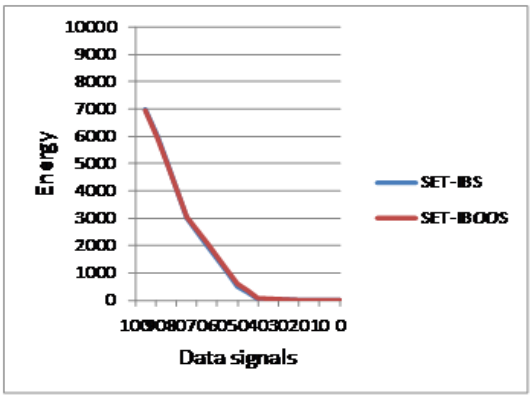

Fig 4: Comparison of energy consumption between SET-IBS and SET-IBOOS protocols

Figure 4 show the energy value reaches to zero when the power of the signal is stronger compared to that of noise. In both SET-IBS and SET-IBOOS method, energy consumption value has reached to zero. This is one of the strongest parameter that helps in efficient transmission of data by minimizing energy consumption.

4.2 Network Life Time (FND)

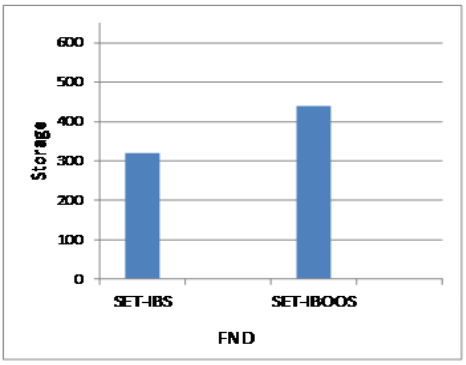

Fig 5: Comparison of FND time between SET-IBS and SET-IBOOS

Figure 5 exposed that the time of first node dies (FND), indicates the length that the sensor network is fully functional. So, maximizing the time of FND in a WSN is to extend the network lifetime

4.3 Bit Error Rate

Bit errors is the number of received data bit stream over a communication channel that have been changed due to sound, interference, bend or bit synchronization errors.

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

Where, BER is Bit Error Rate

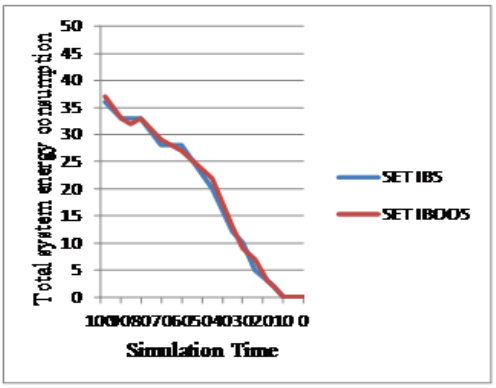

Fig 6: comparison of BER of SET-IBS and SET-IBOOS

In figure 6, the bit error rate for both the IBS and IBOOS method is shown. Here in the beginning of bit error rate for IBS technique is more compared to that of IBOOS but as the strength of the signal increases compared to that the value of bit error rate reaches to zero as shown in the figure.

In both SET-IBS and SET-IBOOS method energy consumption value reaches zero. This, one of the strongest parameter that helps in efficient transmission of data by minimizing energy consumption. In this security is based on digital signature for that, we use two protocol SET-IBS and SET-IBOOS. Using this protocol the attackers can be recognized easily. In CWSNs multi hop data transmission is used flanked by the CH to BS, where direct communication is not likely due to distance. By using this method, we can reduce the energy consumption in SET-IBS and SET-IBOOS.

6. Conclusion

In this paper, we converse that the wireless sensor network is secure and efficient. This security is based on digital signature. Wireless sensor networks are more useful for various areas like medical, military, money-making applications, environmental. This approach should have some difficulties like taking more time to process. In future, we will try to trim down the time using SET-IBS and SET-IBOOS protocol with various algorithms. Adding security to protocols is difficult, because they dynamically, and periodically rearrange the network ‘s clusters and data links. So in future, we will to solve that problem also.

Reference

[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] Huang Lu, “Secure and efficient data transmission Cluster-Based wireless Sensor Network “Jie Li Senior Member IEEE Transaction on Parallel and distributed System, March 2014.

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

[4] 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.
[5] 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.
[6] 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.
[7] A. Shamir, "Identity - Based Cryptosystems and Signature Schemes," in Lect. Notes. Comput. Sc. - CRYPTO, 1985, vol. 196, pp. 47–53.
[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] S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," in Proc. ICCCS, 2011, pp.146–151.