International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 25th Oct 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-11

Title: **CLUSTER-BASED WIRELESS SENSOR NETWORKS FOR SECURE DATA TRANSMISSION TECHNIQUES**

Volume 07, Issue 11, Pages: 39–44.

Paper Authors

N.VIDYASAGAR, S.S.N ANJANEYULU
Eswar College of Engineering, Narasaraopet, Guntur.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

CLUSTER-BASED WIRELESS SENSOR NETWORKS FOR SECURE DATA TRANSMISSION TECHNIQUES

N.VIDYASAGAR[1], S.S.N ANJANEYULU[2]
[1] Research Scholar, Eswar College of Engineering, Narasaraopet, Guntur.
[2] Asst. Professor & Research Supervisor, Eswar College of Engineering, Narasaraopet, Guntur.

Abstract—secure data transmission is a main issue for wireless sensor networks (WSNs). Clustering is an efficient and practical way to enhance the system improvement of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Index Terms—Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission protocol.

Introduction

In the Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings. In this Proposed System, Secure and Efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Ofline digital Signature (IBOOS) scheme, respectively. It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are Efficient in communication and applying the key management for security. In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

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, secures 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.

3. SYSTEM DESIGN

In this section, the below given are the explanation of block diagram design and the proposed system explanation is as followa

A. Proposed solution

The main objective of the proposed work is to provide security for the data in wireless network as the data is to be send 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 decreased 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.

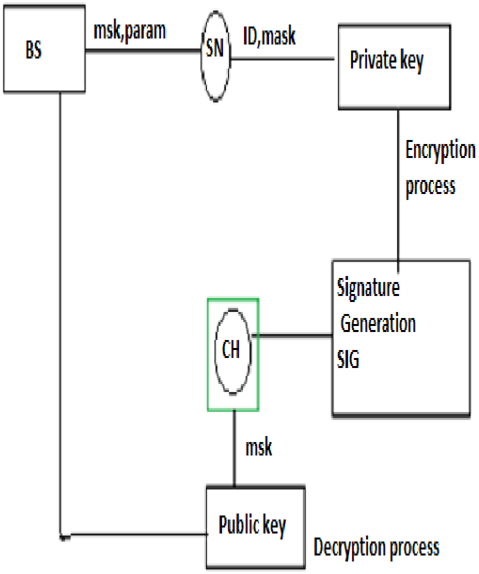

Fig 1: Workflow of SET-IBS protocol

Workflow of SET-IBOOS and its Operation

SET-IBOOS is proposed in order to further decrease the computational overhead for security using the IBOOS technique, 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.

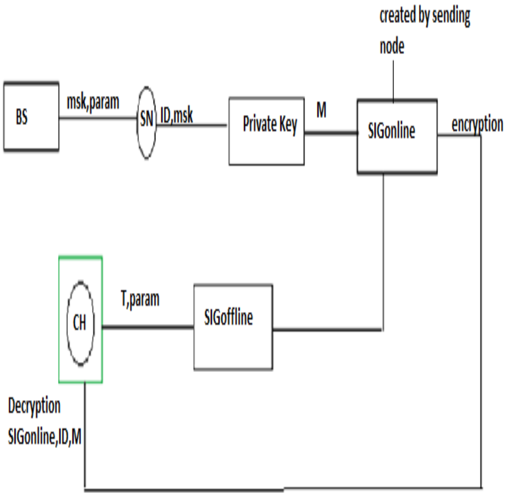

Fig 2: Workflow of IBOOS protocol

4. Simulation Results

In this work we have developed a sensor network model in Mat lab to incorporate Phy-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. 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

$$Ebs\ (Kc) = -1/\ K_C(1+\ \alpha)\ N_f\ \sigma^2 \ln(P_b)\ G_1M^2M_1+Pct+Pcr/B$$

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.

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

- Signal to noise ratio (SNR): The ratio of the strength of electrical or other signal carrying information to that of unwanted interference.
- 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.

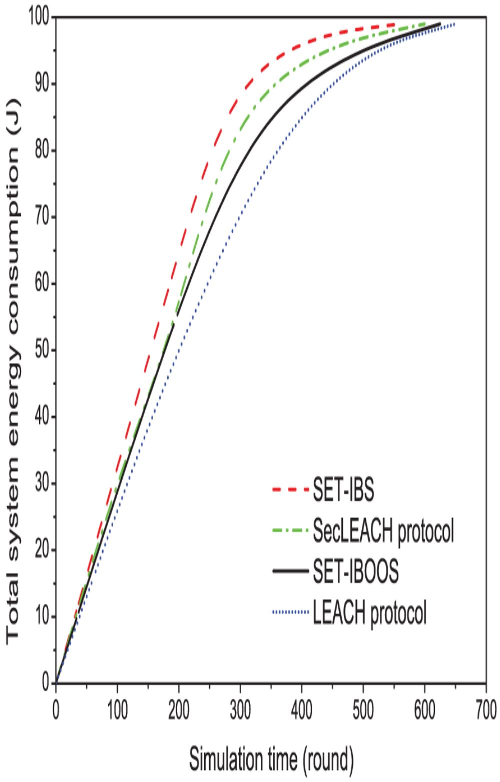

Fig 3 graphs showing the comparison of energy consumption of SET- IBS and SET-IBOOS

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. 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. The security provided by IBOOS technique is more as compared to that of IBS.

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.

AUTHORS PROFILE

N.VIDYA SAGAR is a student pursuing MTech(CSE) in Eswar college Of Engineering, Narasaraopet, Guntur.

S.S.N Anjaneyulu M.Tech in Computer Science & Engineering. He is presently working as an Asst. Prof. in Eswar College of Engineering, Narasaraopet, Guntur, India. He is having about 6 years of teaching experience in different Engineering Colleges. He published 02 international journals. and attended 1 international conference He attended ISTE workshop on "**Data Base Management**

Systems” conducted by IIT Bombay. He also attended Two weeks workshop on “**Entrepreneurship Development**” conducted by NIMSME.