International Journal of Advance Research in Science and Engineering
Vol. No.5, Special Issue No. (01), February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

TO IMPLEMENT SECURE IDENTITY-BASED SET-IBS AND SET-IBOOS SCHEMES FOR CLUSTER-BASED WIRELESS SENSOR NETWORKS

S.Amsapriya[1] D.Geetha[2]

[1]PG Scholar, [2]Assistant Professor, Department of CSE,
Adhiyamaan College of Engineering, Hosur, Tamil Nadu, (India)

ABSTRACT

Clustering is an effective and practical way to enhance the system performance of Wireless Sensor Networks (WSNs). In WSNs, it is highly a difficult task to achieve secure data transmission. In existing system, some of the protocols such as SecLEACH, GS-LEACH, and RLEACH were used, but orphan node problem exists. Thus by using these protocols, the orphan node problem is solved due to node-to-node communication. Secure data transmission for Cluster-based WSNs (CWSNs) can be provided with help of protocols. In proposed system, two secure and efficient data transmission protocols namely SET-IBS and SET-IBOOS scheme were proposed were proposed SET-IBS has a protocol initialization prior to the deployment and operates in round communication. SET-IBOOS operates similarly to the previous SET-IBS. The feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirement and security analysis various attacks. In this paper, a modified protocol SET-IBS has proposed that formed dynamically, randomly and periodically. Thus the probability of two nodes will share a key to orphan rate of the orphan node problem. SET-IBOOS system lifetime will be increased. The time of FND in both SET-IBS is shorter than of LEACH protocol due to the security overhead on computation cost of the IBS process.

Keywords: CWSNs ,GS-LEACH, RLEACH, SecLEACH, SET-IBS, SET-IBOO,WSNs.

I. INTRODUCTION

A WSN is a network structure where the devices are spatially distributed using wireless sensor nodes. These wireless sensor nodes are used to monitor environmental or physical conditions, such as pressure, motion, sound, temperature etc. These nodes are capable of sensing their environmental conditions, process the information data, and sending data to one or more points in a WSN. The deployment of wireless sensor nodes was motivated by military applications such as battle-surveillance, many industrial and commercial applications. Often the deployment of wireless sensor nodes in adversary, neglected and harsh systems causes a great threat to the society. Transmission of data in secure and efficient manner is one of the most critical issues for WSNs. Secure and efficient data transmission is very much necessary. This has been demanded in many practical WSNs. Network scalability and management maximizes node lifetime and reduces bandwidth consumption by using local collaboration among sensor nodes. In order to achieve this, data transmission based on clusters has been investigated.

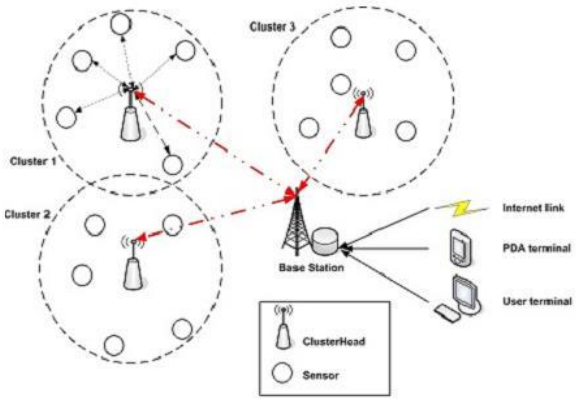

Fig 1: Cluster based WSN

II.BACKGROUND AND MOTIVATION

Several cluster based protocols were introduced. In cluster based WSN every cluster has a leader sensor node. This is termed as CH. The data collected by the leaf nodes in the cluster are aggregated by the cluster head. The cluster head sends the aggregated-data to the BS (Base Station).

The LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a well-known hierarchical protocol. It is very effectively used to minimize and balance the total consumption of energy for CWSNs. LEACH achieves significant improvements in terms of network lifetime. Based on the idea of LEACH, a number of protocols have been introduced such as APTEEN and PEACH. They used similar concepts in LEACH. These category of cluster-based protocols are called as LEACH-like protocols. In the last decade CWSNs have been widely studied by the researchers. However, the implementation of the architecture based on clusters in the real world is rather complicated. LEACH-like protocols periodically, dynamically and randomly rearrange the data links and clusters in the network. Hence adding security to LEACH-like protocols is a challenge. Therefore in LEACH like protocols, providing common key distributions and long lasting node-to-node trust relationships steadily are inadequate. Sec LEACH, GS-LEACH and RLEACH are some of the secure data transmission protocols. These protocols are based on LEACH. These protocols however, make use of symmetric key management for security. They suffer from the orphan node problem. A pairwise key is not shared by the node with the other nodes in its key-ring preloaded. Hence in a network the key ring is not sufficient for the node to share symmetric keys with all of the nodes. Such nodes cannot participate in any cluster. Hence it has to elect itself as the CH(Cluster Head). When there are more number of CHs elected by themselves the overall energy consumed is more. This results in the increase in the overhead of transmission and energy consumption of the system. It requires comparatively high amount of energy for a sensor node to transmit data to the distant CH. Nowadays asymmetric management has been found feasible for WSNs in comparison to symmetric management for security. In asymmetric key management systems digital signature is one of the most important security services offered by cryptography. There is a bond between the public key and the signer identification. This is obtained via a digital certificate. Recently, the technique of IBS and IBOOS has been developed for secure and efficient transmission of data. As a key management for security, IBS has been developed in WSNs. In order to decrease

the storage costs and computation of signature processing the IBOOS scheme has been developed. A general technique for online-offline schemes for signature was introduced. The offline phase executes on a node or at the BS before communication. The online phase executes during communication.

III.RELATED WORK

In [1], the authors study a secure data transmission for cluster based WSNs (CWSNs), where the clusters are formed dynamically and periodically. The author 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. The authors 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.

In [3], different hierarchical routing algorithms are studied. These algorithms are analyzed and compared based on various criteria. This evaluation is very useful for researchers to implement security in hierarchy protocol.In [4], the problem of authentication has been discussed. A secure and efficient framework has been proposed for authentication. Online/offline signature scheme authentication scheme was found to be a solution.In [5], the notion of online/offline ID-based signcryption" was redefined and provided a scheme that realizes it. The construction is very efficient. This means that it does not require any pairing operation in the stages of online and online signcryption. Furthermore, the receiver's information is not required in the online signcryption stage. It is thefirst in the literature to remove such requirement. Without this restriction, this scheme is more flexible and practical.The scheme is particularly suitable to provide authentication and confidentiality to power constrained communication devices. A practical solution is needed to provide secure and authenticated transaction for smart cards or mobile devices such as smart phone. In [6], a survey of issues related to security in wireless sensor networks is done. WSN suffers from many constraints like small memory, low computation capability, limited energy resources and use of insecure wireless communication channel. There are 5 security issues: Key management, cryptography, secure data aggregation, secure routing and intrusion detection. The various advantages and disadvantages of protocols in WSNs are discussed. The security services discussed add more computation, storage overhead and communication. The significance of wireless sensor networks and its applications have been explained in [7]. A survey of various clustering schemes has been done. The clustering schemes are classified based on their objectives, characteristics, properties, processes. The strengths and limitations of the clustering schemes are also discussed. The clustering schemes are compared based on metrics like rate of convergence, stability, overlapping etc. In [8], the recent advances in technology have made it likely to have small sensor devices with low power. They are equipped with multiple parameter sensing, wireless communication capability and programmable computing. But, because of their built-in limitations, the protocols constructed for such WSNs must efficiently use both battery energy and limited bandwidth. The M/G/1 model

was developed to determine the delay analytically, suffered in handling various types of queries. This was performed using improved protocol named APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network).In wireless sensor networks (WSNs), the important issues are gathering sensed information data, transforming the sensed information data to the BS in an efficient manner, and increasing the lifetime of the network. Clustering is an efficient way that groups sensor nodes into many clusters. In [9], author proposes PEACH protocol, which is a power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks. By using over hearing 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 [10], Cluster-based communication has been addressed for these networks for various reasons such as scalability andenergy 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 [11], 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.

IV.METHODOLOGY & ALGORITHM

4.1 IBS Scheme for Cwsns

• **Setup** - The BS generates a master key and public parameters and distributes to all sensornodes.
• **Extraction** - sensor node generates a private key using ID and master key.
• **Signature signing** - for the msg M, time stamp‘t’, sending node generates the signature.
• **Verification** - the receiving node verifies and outputs “accept” if signature is valid otherwise outputs “reject”.

4.2 Iboos Scheme for Cwsns

• **Setup** - The BS generates a master key and public parameters and distributes to all sensor nodes.
• **Extraction** - sensor node generates a private key using ID and master key.
• **Offline signing** - for given public parameters and time stamp ‘t’, the CH node generates the offline signature
• **Online signature** - from private key, SIGoffline and M, a sending node generates SIGonline.
• **Verification** - the receiving node verifies and outputs “accept” if SIGonline is valid otherwise outputs “reject”.

4.3 The multihop planar model:

Multihop data transmission is used for transmission between the CHs to the BS, where the direct communication is not possible due to the distance or obstacles between them. The version of the proposed SET-IBS and SET-IBOOS protocols for CWSNs can be extended using multihop routing algorithms, to form secure data transmission protocols for hierarchical clusters. A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data are sent to the BS. We have proposed an energy-efficient routing algorithm for hierarchically clustered WSNs and it is suitable for the proposed secure data transmission protocols. Mulithop

algorithm always chooses the path to the destination within the minimum number of hops. It is the simplest multi hop algorithm, which is trying to minimize the total transmission time.

4.4 The cluster-based hierarchical method

Clusters are the organizational unit for WSNs. The dense nature of these networks require the need for them to be broken down into clusters to simplify tasks such a communication. The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user. The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS. The decision of whether a node elevates to cluster head is made dynamically at each interval. The elevation decision is made solely by each node independent of other nodes to minimize overhead in cluster head establishment.

V. PROPOSED PROTOCOLS CHARACTERISTICS

In this part, we summarize the characteristics of the proposed SET-IBS and SET-IBOOS protocols. Table IV shows a general summary of comparison of the characteristics of SET-IBS and SET-IBOOS with prior ones, in which metrics are used to evaluate whether a security protocol is appropriate for CWSNs. We explain each metric as follows.

- **Key Management:** the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.
- **Neighborhood Authentication:** used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, “limited” means the probability of neighborhood authentication, where only the nodes with the shared pair wise key can authenticate each other.
- **Storage Cost:** represents the requirement of the security keys stored in sensor node’s memory.
- **Network Scalability:** indicates whether a security protocol is able to scale without compromising thesecurity requirements. Here, “comparative low” means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network, and vice versa.
- **Communication Overhead:** the security overhead in the data packets during communication.
- **Computational Overhead:** the energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.
- **Attack Resilience:** the types of attacks that security protocol can protect against.

V1. IDENTITY BASED SCHEME

The feasibility of the asymmetric key management has been used in WSNs recently, which compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate.

6.1 SET-IBS

The identity-based digital signature (IBS) scheme, based on the difficulty of factoring integers from identity-based cryptography (IBC), is to derive an entity's public key from its identity information, for example, from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security

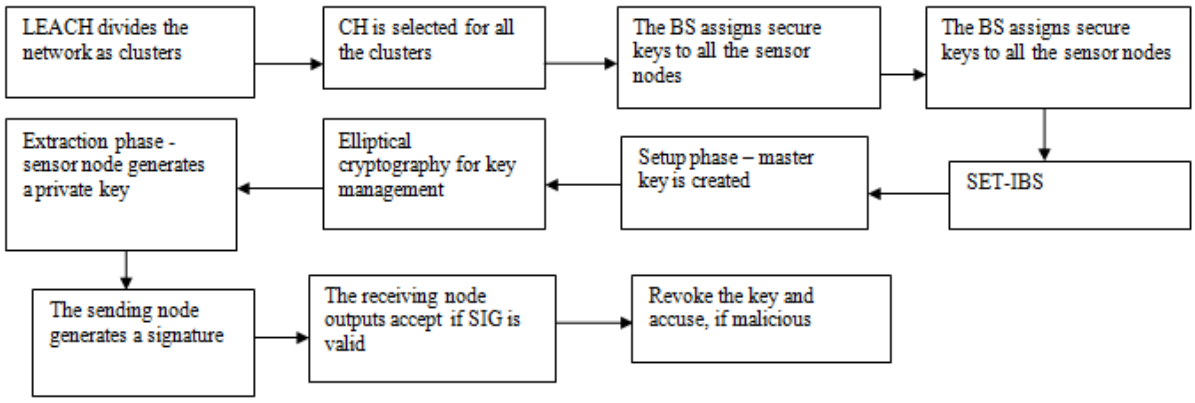

Fig 6.1 System architecture design for SET-IBS.

6.2 SET-IBOOS

The IBOOS scheme has been introduced to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced. The IBOOS scheme could be effective for the key management in WSNs. Specifically; the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

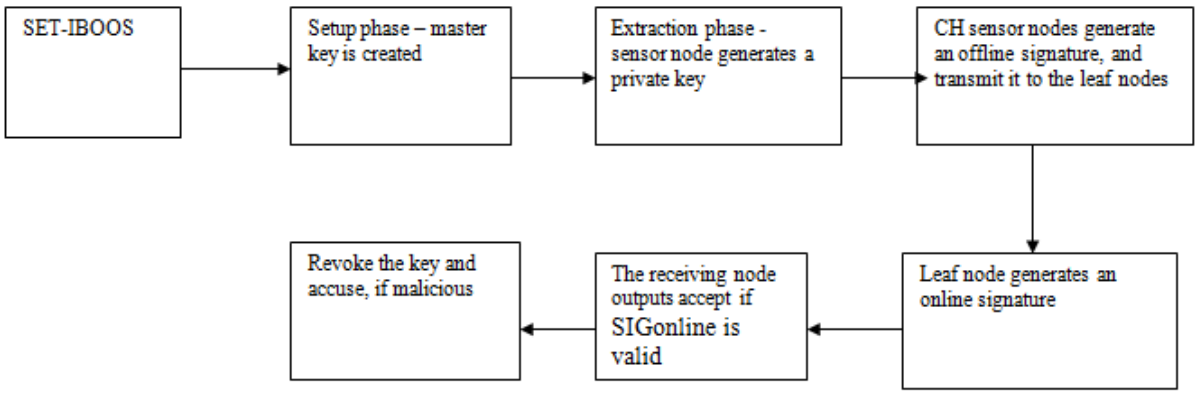

Fig 6.2 System architecture design for SET-IBOOS

The advantages of identity based scheme are:

- The key idea of both SET-IBS and SET-IBOOS is 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 Identity Based Scheme , secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes key escrow problem described in ID-based cryptosystems
- Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

- SET-IBOOS is introduced to further reduce the computational overhead for security using the IBOOS scheme.
- Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with asymmetric key management.
- The Identity Based Scheme with respect to the security requirements and analysis against three attack models such as active attack, passive attack, compromising attack.

VII. SIMULATION RESULTS

Comprehending the extra energy consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed SET-IBS and SETIBOOS. To evaluate the energy consumption of the computational overhead for security in communication, we consider three metrics for the performance evaluation: Network lifetime, system energy consumption, and the number of alive nodes. For the performance evaluation, we compare the proposed SET-IBS and SET-IBOOS with LEACH protocol and SecLEACH protocol :

- **Network lifetime (the time of FND):** We use the most general metric in this paper, the time of first node dies (FND), which indicates the duration that the sensor network is fully functional. Therefore, maximizing the time of FND in a WSN means to prolong the network lifetime.
- **The number of alive nodes:** The ability of sensing and collecting information in a WSN depends on the set of alive nodes (nodes that have not failed). Therefore, we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network.
- **Total system energy consumption:** It refers to the amount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols. In the network simulation experiments, 100 nodes are randomly distributed in a 100 m ×100 m area, with a fixed BS located near part of the area, as shown in the figure in the Appendix. All the sensor nodes periodically sense events and transmit the data packet to the BS. We assume that the sensor CPU is a low-power high-performance Intel PXA255 processer of 400 MHz, which has been widely used in many sensor products, for example, Crossbow Stargate.

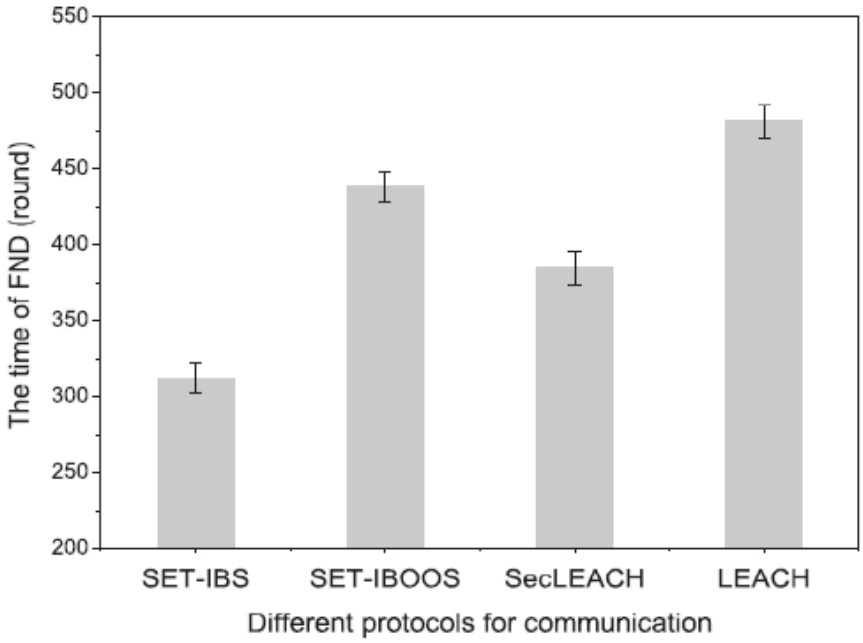

Fig 7.1 Comparison of FND time in different protocols.

Fig.7.1 illustrates the energy of all sensor nodes disseminated in the network, which also indicates the balance of energy consumption in the network. the comparison of alive nodes' number, in which the proposed SET-IBS and SET-IBOOS protocols versus LEACH and SecLEACH protocols. The results demonstrate that the proposed SET-IBS and SET-IBOOS protocols consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS or IBOOS process. However, the proposed SET-IBOOS has a better balance of energy consumption than that of SecLEACH protocol.

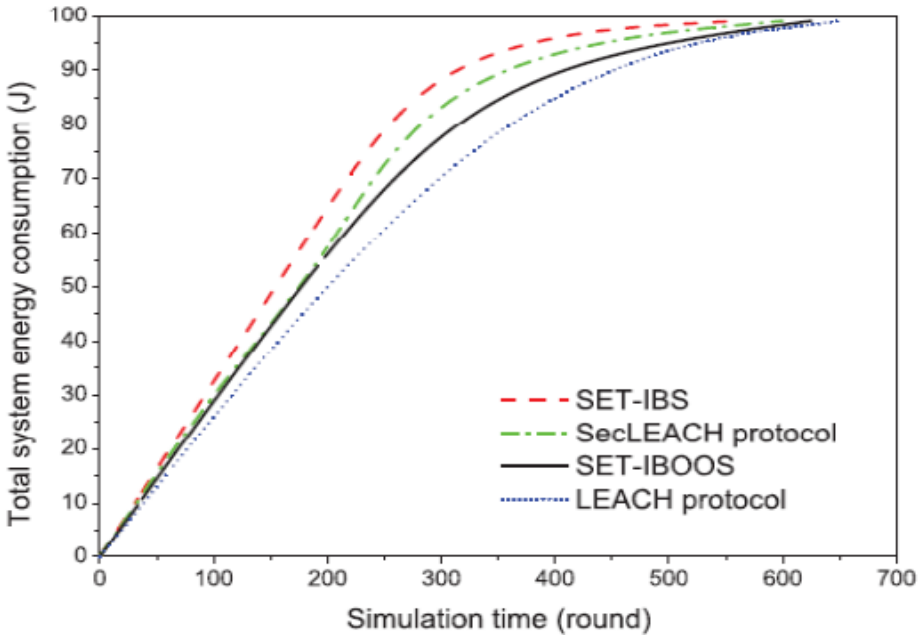

Fig.7.2 Comparison of energy consumption in different protocols.

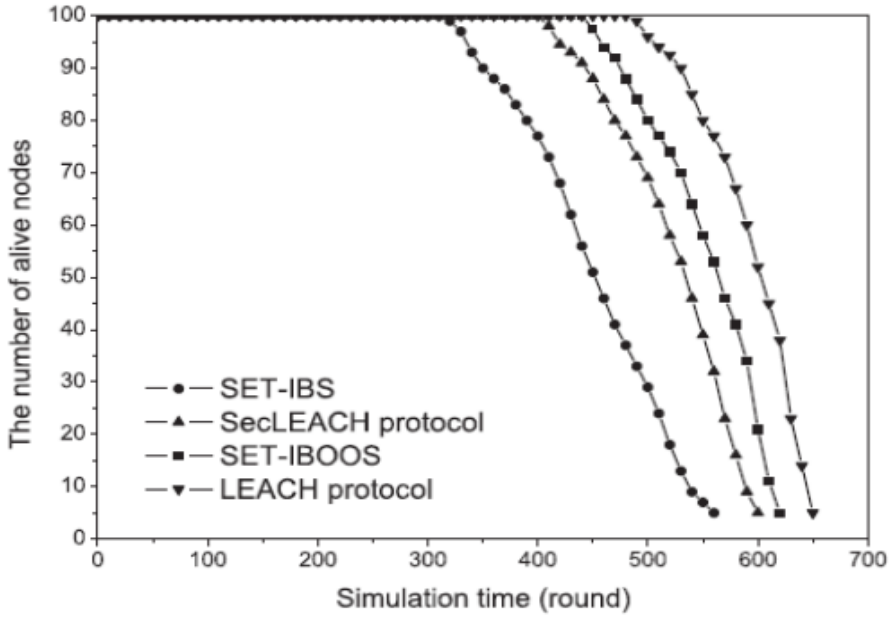

Fig.7.3. Comparison of the number of alive nodes in different protocols

.

VIII. CONCLUSION

In this paper, a secure data transmission for cluster-based WSNs(CWSNs), where the clusters are formed dynamically and periodically. We proposed two secure and efficient data transmission (SET) protocols for CWSNs,called SET-IBS, and SET-IBOOS, by using the identity-based digitial 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 futher reduces the computational overhead for protocol security, which its crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. They show the feasibility of the SET-IBS and SET-IBOOOS protocol with respect to the security requirement and security analysis against various attacks. The result show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

ACKNOWLEDGMENT

This is a great pleasure and immense satisfaction to express my deepest sense of gratitude and thank to everyone who has directly or indirectly helped me in this project work successfully.

REFERENCES

[1] A.A. Abbasi and M.Younis," A Survey on Clustering Algorithm for Wireless Sensor Networks," Computer Comm., vol.30,nos. 14/15,pp. 2826-2841, 2007.

[2] D. Boneh and M.Franklin," Identity-Based Encryption from the Weil pairing," proc. 21st Ann.Int'1 cryptology Conf. Advances in Cryptology(CRYPTO '01), pp. 213-229,2009.

[3] D.W Carman," New Directions in Sensor Network Sensor Networks Key Mangement," Int'1 J.Distributed Sensor Network, vol. 1,pp. 3-15,2005.

[4] H. Lu, J. Li, and H.Kameda," A Secure Routing Protocols for Cluster-Based Wireless Sensor Networks using ID-Based Digital Signature," Proc. IEEE GLOBECOM, pp. 1-5, 2015.

[5] A. Manjeshwari, Q-A. Zeng, and D.P. Agrawel, "An Anallytical Model for information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed System, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] L.B. Oliveria et al., " SecLEACH On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882- 2895, 2007.

[7] K.Pradeepa, W.R. Anne, and S. Duraisamy," Desgin and Implementation Issues of Clustering in Wireless Sensor Networks," Int'1 J.Computer Application, vol. 47, no.11, pp. 23-28, 2012.

[8] A.Shamir,"Identity-Based Cryptosystem and Signature Schemes," Proc. Advances in cryptology(CRYPTO), pp. 47-53, 1985.

[9] S.Sharma and S.K. Jena," A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'1 Conf. Comm., Computing & Security (ICCCS), pp.146-151,2011.

[10] S.Yi et al., "PEACH:Power-Efficient and Adaptive Clustering Hierarchy Protocols for Wireless Sensor Networks," Computer Comm., vol. 30,nos. 14/15, pp. 2842-2852, 2007.

[11] R. Yasmin, E. Ritter, and G.Wang," An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signature," Proc. IEEE Int'1 Conf. Computer and Information Technology(CIT),pp.882-889, 2010.

[12] S.Xu, Y. Mu, and W.Susilo,"Online/Offline Signature and Multisignature for AODV and DSR Routing Security," proc. 11th Australasian Conf. Information Security and Privacy, pp 99-110, 2006.