Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 2, May 2015

Providing Security and Efficiency for the Transmission of data in Cluster-Based Wireless Sensor Networks

Chaitrashree H.M.[1]
4th sem Mtech in Computer Networks and Engineering
Akshaya Institute of Technology
Tumkur,India
Phone no: 8147575834

Mr.Yashwanth T.R[2]
Asst prof,Dept of Computer Science and Engineering
Akshaya Institute of Technology
Tumkur,India
Phone no:9916643435

***Abstract*:**Wireless Sensor Networks (WSN) are emerging asboth an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc.

Clustering is an effective and practical way to enhance the system performance of WSNs. Secure data transmission is a critical issue for WSNs. To obtain the secure and efficient data transmission the two protocols i.e.., SET-IBS(Secure and Efficient data Transmission-Identity Based digital Signature), SET-IBOOS(Secure and Efficient data Transmission-Identity Based Online/Offline digital Signature) are designed. These provides the security requirements and security analysis against various attacks, and also provide better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Keywords: *wireless sensor networks(WSN),SET-IBS,SET,IBOOS, Performance, Security overhead, Energy consumption and Base Station (BS).*

1.INTRODUCTION

In these days, wireless sensor network emerging as a promising and interesting area. Homogeneous and Heterogeneous nodes are used in wireless sensor network where a wireless medium is used by the nodes to communicate with each other. A hundred to thousands of nodes can be deployed in the sensing region to sense the environment. These nodes work cooperatively and send sensed information to the sink. Wireless sensor network can be categorized into two types 1 Unstructured WSN- The nodes are densely deployed and also the nodes can be deployed in ad-hoc manner in the sensing area or region. 2 Structured WSN – Sensor node developments of some or all nodes are preplanned. The nodes placement is also planned. So, the maintenance of structured WSN is much easy as compare to Unstructured WSN [1]. Sensor nodes work cooperatively to monitor environment conditions such as temperature, sound, vehicular movement, pressure and pollutants. The sensor nodes are deployed in the sensing area through wireless links which provide opportunities for many civilian and military applications, for example: intrusion detection, battlefield monitoring and availability of equipments, environment observation and home intelligence. A wireless sensor network (WSN) is always assumed a cooperative environment. We cannot rely on this assumption when attacks are imminent like in military applications. Sensor networks are susceptible to attacks at the routing layer, which are related to node behaviour. The most familiar attacks are non-forwarding attacks in which a compromised node will drop the packets that it receives instead of forwarding them [1]. Such attacks cannot be detected or avoided by identity checkingmechanisms. Hence, behaviour trust should be implemented in order to defend against these attacks. We define 'trust' as the level of confidence that a node has in its neighbor'scooperation [2]. This trust can be attained following two broad approaches: centralized or distributed. The centralizedapproachassumes a central agent that can assess the'credibility' of each node and then disseminate this information to all 'real'nodes.It is obvious thatsuch anapproach is difficult to realize in practice. On the other hand, the distributed approach is a localized scheme where each node assesses the credibility of its neighboring nodes and accordingly builds its trust-aware routing. This process of defining the trust levels for every sensor node in the network and then obtaining a trust-aware routing is called reputation. A reputation system is a type of cooperative filtering algorithm, which attempts to determine ratings for a collection of entities that belong to the same

entities of interest based on a given collection of opinions that those entities hold about each other [3]. In the context of MANET and WSN, the reputation of a node is the amount of trust the other nodes grant to it regarding its cooperation andparticipation in forwarding packets [3]. Hence, each node keeps track of each other's reputation according to thebehaviour it observes, and the reputation information that may be exchanged between nodes to help each other infer the accurate values. In this work, they proposed a reputation system solution for trust-aware routing, which implements a new monitoring strategy called Efficient Monitoring Procedure In Reputation system (EMPIRE). EMPIRE tries to solve the problem of efficient monitoring in a WSN. Monitoring efficiency is realized here by the association between the nodal monitoring activity (NMA) and various performance measures. The feasibility of asymmetric key management has been shown in WSN , which compensates the shortage of 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 by the digital certificate.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 eg, from its name or ID number. Recently the concept of IBS has been developed as a key management in WSNs for security. Carman the first who combined the benefits of IBS and predistribution set into WSNs . The IBOOS scheme has been proposed to reduce the computation and storage costs of signature processing. A general method for constructing online/ offline signature is introduced by Even et al. 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,The offline signature in these schemes,however,is precompued by a third party and lacks reusability,thus they are not suitable for CWSNs.

1. IBS AND IBOOS FOR CWSNs

In this section, we introduce the IBS scheme and IBOOS scheme used in the paper. Note that the conventional schemes are not specifically designed for CWSNs. We adapt the conventional IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes, based on at first. To further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs, .

In a finite cyclic group G of prime order q, there exists an element g as the generator and elements g^x 2 G, such that G ¼ hgi ¼ fg^x j x 2 Z^-_q ¼ f1; 2; . . . ; q _ 1gg, where Z^-_q is a multiplicative group consisting of q _ 1 integers, in which the multiplication operation in the group ends in the remainder on the division by q (mod q) [25]. The discrete logarithmproblem (DLP) [26] in the cyclic group G is to compute x, in which the computational complexity is believed to be hard, where the security in the IBOOS scheme is based on the DLP in this work.

2.1IBS Scheme for CWSNs

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes:

- Setup. The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
- Extraction. Given an ID string, a sensor node generates a private key sek_{ID} associated with the ID using msk.
- Signature signing. Given a message M, time stamp t and a signing key _, the sending node generates a signature SIG.
- Verification. Given the ID, M, and SIG, the receiving node outputs "accept" if SIGis valid, and outputs "reject" otherwise.

2.2 IBOOS Scheme for CWSNs

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes:

- Setup. Same as that in the IBS scheme.
- Extraction. Same as that in the IBS scheme. Offline signing. Given public parameters and time stamp t, the CH sensor node generates an offline signature $SIG_{offline}$, and transmit it to the leaf nodes in its cluster.
- Online signing. From the private key sek_{ID}, $SIG_{offline}$ and message M, a sending node (leaf node) generates an online signature SIG_{online}.
- Verification. Given ID, M, and SIG_{online}, the receiving node (CH node) outputs "accept" if $SIG_{online}$is valid,and outputs "reject" otherwise.

3. THE PROPOSED SET-IBS PROTOCOL

The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialisation, describe the key management of the protocol by using the IBS scheme, an protocol operations.

3.1PROTOCOL INITIALIZATION

In SET-IBS time is divided into intervals.In this paper, we adopt IDkt as user's public key under an IBS scheme [24], and propose a novel secure data transmission protocol by using IBS specifically for CWSNs (SET-IBS). The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this way, when a sensor node wants to authenticate itself to another node, it does not have to obtain its private key at the beginning of a new round. Upon node revocation, the BS broadcasts the compromised node IDs to all sensor nodes, each node then stores the revoked IDs within the current round. We adopt the additively homomorphic encryption scheme in [29] to encrypt the plaintext of sensed data, in which a specific operation performed on the plaintext is equivalent to the operation performed on the ciphertext. Using this scheme allows efficient aggregation of encrypted data at the CHs and the BS, which also guarantees data confidentiality. In the protocol initialization, the BS performs the following operations of key predistribution to all the sensor nodes:

- Generate the encryption key k for the homomorpic encryption scheme to encrypt the data messages.
- Generate the pairing parameters.
- Choose the cryptographic hash functions.
- Pick a random integer as the master key.
- Preload each sensor node with the system parameters.

3.2 KEY MANAGEMENT FOR SECURITY

Assume that a leaf sensor node j transmits a message M to its CH i, and encrypts the data using the encryption key k from the additively homomorphic encryption scheme [29]. We denote the ciphertext of the encrypted message as C. We adapt the algorithms of the IBS scheme from [24] to CWSNs practically and provide the full algorithm in the signature verification, where security is based on the DHP in the multiplicative group. The IBS scheme in the proposed SET-IBS consists of following three operations: extraction, signing, and verification is done here.

3.3 PROTOCOL OPERATION

After the protocol initialization, SET-IBS operates in rounds during communication .Each round consists of setup and steady phase. We suppose that all sensor nodes know the starting and ending time of each round because of the time synchronization.

The operation of SET-IBS is divided by rounds as shown in Fig. 1, which is similar to other LEACH-like protocols. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS. In each round, the timeline is divided into consecutive time slots by the TDMA control [4]. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly elected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. To elect CHs in a new round, each sensor node determines a random number and compares it with a threshold. If the value is less than the threshold, the sensor node becomes a CH for the current round. In this way, the new CHs are self-elected based by the sensor nodes themselves only on their local decisions; therefore, SET-IBS functions without data transmission with each other in the CH rotations.

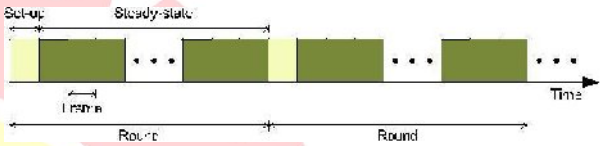

Fig. 1. Operation in the proposed secure data transmission.

The operation of SET-IBS is divided by rounds as shown in Fig. 1, which is similar to other LEACH-like protocols. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS. In each round, the timeline is divided into consecutive time slots by the TDMA control [4]. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly elected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. To elect CHs in a new round, each sensor node determines a random number and compares it with a threshold. If the value is less than the threshold, the sensor node becomes a CH for the current round. In this way, the new CHs are self-elected based by the sensor nodes themselves only on their local decisions; therefore, SET-IBS functions without data transmission with each other in the CH rotations.

4. THE PROPOSED IBOOS PROTOCOL

We present the SET protocol for CWSNs by using IBOOS (SET-IBOOS) in this section. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SET-IBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operationafterward.

Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 2, May 2015

4.1 PROTOCOL INITIALIZATION

To reduce the computation and storage costs of signature signing processing in the IBS scheme, we improve SET-IBS by introducing IBOOS for security in SET-IBOOS. The operation of the protocol initialization in SET-IBOOS is similar to that of SET-IBS; however, the operations of key predistribution are revised for IBOOS. The BS does the following operations of key predistribution in the network:

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages.
- Let G be a multiplicative finite cyclic group with order q. The PKG selects a random generator g of group G generation, and chooses the number randomly as the master key .
- For each node j, randomly select r_j 2 Z^{-}_{q} for its private key generation, and let H be a hash function.
- Preload each sensor node j with the public parameters.

4.2 KEY MANAGEMENT FOR SECURITY

Assume that a leaf sensor node j transmits a message M to its CH i, and we denote the ciphertext of the encrypted message as C_j, which is encrypted by the same encryption scheme in SET-IBS. We adapt the algorithms from [21] to construct an IBOOS scheme for CWSNs, where security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during theprotocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations: extraction, offline signing, online signing, and verification are done here.

4.3 PROTOCOL OPERATION

The proposed SET-IBOOS operates similarly to that of SET-IBS. SET-IBOOS works in rounds during communication, and the self-elected CHs are decided based on their local decisions, thus it functions without data transmission in the CH rotations.

However, the differences are the digital signatures that are changed from the ID-based signatures to the online signatures of the IBOOS scheme.

Once the setup phase is over, the network system turns into the steady-state phase, in which data are transmitted to the BS. The steady-state operates where the ID-based signatures are changed into the online signatures of the IBOOS scheme.

5. PROPOSED ARCHITECTURE

The study propose two secure and efficient data transmission protocols for wireless sensor network considering both online and offline interaction vulnerabilities from the adversary using identity based cryptography scheme. The novelty of the approach is that till now few studies are focussed on online and offline vulnerabilities in wireless sensor network. The prime idea of proposed system is to perform authentication of 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, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the base station initially, which overcomes the key escrow problem in identity based cryptosystems Secure communication using the proposed study will rely on the identity based cryptography, in which, user public keys are their identity information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

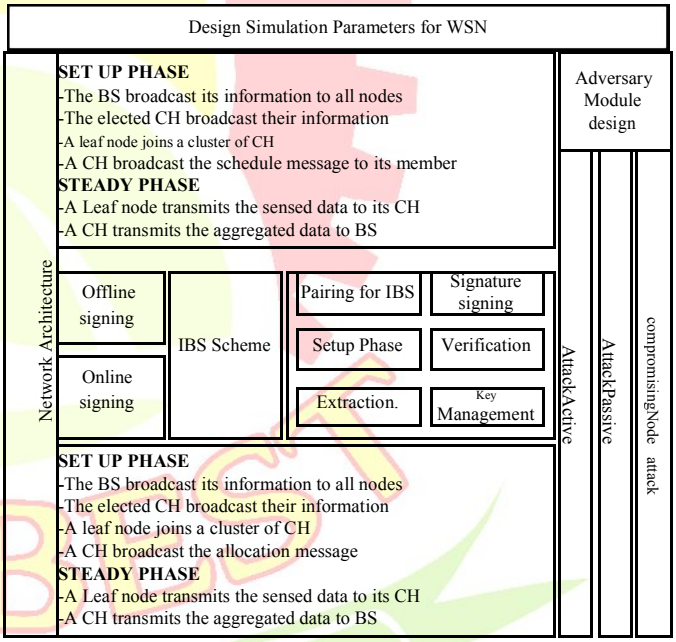

Fig 2: Indicative Architecture of Proposed System.

The system will be designed to further reduce the computational overhead for security using the online and offline scheme, in which security relies on the hardness of the discrete logarithmic problem. The proposed system is also targeted to solve the orphan node problem in the secure data transmission with a symmetric key management. The study also shows the feasibility of the proposed protocols with respect to the security requirements and analysis against novel attack models to be designed. The operation is carried out in this pattern. The proposed framework has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase

and a steady-state phase in each round.

In proposed system, the offline signature is executed by the aggregator node; thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing. This is particularly useful for conventional wireless sensor network because leaf sensor nodes do not need auxiliary communication for renewing the offline signature. Finally security analysis is done based on passive attack, active attack, and node compromising attack scenario and compared with LEACH algorithm for benchmarking purpose.

6. ISSUES IN CLUSTER BASED WSN

Attack and attacker:

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach is called threat and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk.

Security requirements:

Authentication: As WSN communicates sensitive data whichhelps in many important decisions making. The receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during exchange of control information in the network.

Integrity: Data in transit can be changed by the adversaries.Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident.

Data Confidentiality: Applications like surveillance ofinformation, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.

The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [2], [23]. Especially, attacks to CHs in CWSNs could result in serious damage to the network because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending bogus information toward the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs [23]. It is because CHs are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes (i.e., CH nodes). The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secure transmission protocols for CWSNs in the literature [8], [9], [10], however, apply the symmetric key management for security, which suffers from the orphan node problem that is introduced in Section 1. In this paper, we aim to solve this orphan node problem by using the IDbased cryptosystem that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

The proposed SET-IBS and SET-IBOOS provide different types of security services to the communication for CWSNs, in both setup phase and steady-state phase. Both in SET-IBS and SET-IBOOS, the encryption of the message provides confidentiality, the hash function provides integrity, the nonce and time stamps provide freshness, and the digital signature provides authenticity and nonrepudiation:

Solutions to passive attacks on wireless channel

In the proposed SET-IBS and SET-IBOOS, the sensed data are encrypted by the homomorphic encryption scheme from [29], which deals with eavesdropping. Thus, the passive adversaries cannot decrypt the eavesdropped message without the decryption key. Furthermore, both SET-IBS and SET-IBOOS use the key management of concrete ID-based encryption.

. 7. SIMULATION RESULTS

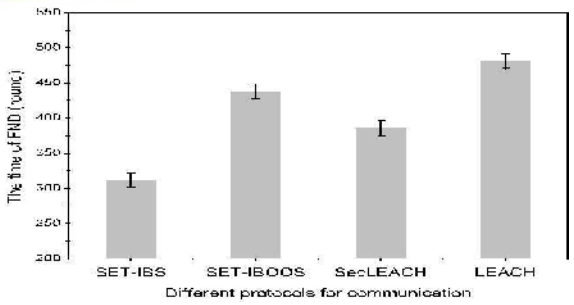

Fig. 3. Comparison of FND time in different protocols

Comprehending the extra energy consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed SET-IBS and SET-IBOOS. 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 [4] and SecLEACH protocol [8]:

- . 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 [1]. 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.

Fig. 3 illustrates the time of FND using different protocols. We apply confidence intervals to the simulation results, and a certain percentage (confidence level) is set to 90 percent. Fig. 5 shows the comparison of system lifetime using SET-IBS and SET-IBOOS versus LEACH protocol and SecLEACH protocol. The simulation results demonstrate that the system lifetime of SET-IBOOS is longer than that of SET-IBS and SecLEACH protocol. The time of FND in both SET-IBS and SET-IBOOS is shorter than that of LEACH protocol due to the security overhead on computation cost of the IBS process.

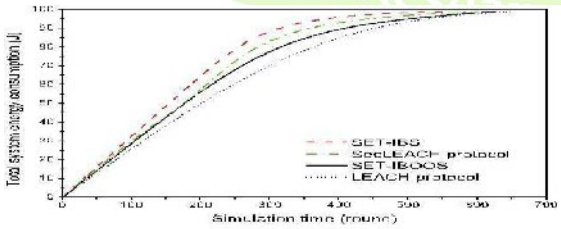

Fig 4: Energy disseminated at all sensor nodes.

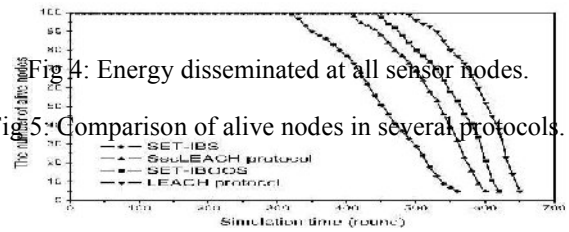

Fig 5: Comparison of alive nodes in several protocols.

Fig. 4 illustrates the energy of all sensor nodes disseminated in the network, which also indicates the balance of energy consumption in the network. Fig. 5 shows 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 commu-nication 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.

8. CONCLUSION

The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based cryptosystem, 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 the calculation and simulation results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computa-tion and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey ofSecurity Issues in Wireless Sensor Networks," IEEEComm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

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

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture forWireless Microsen-sor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "Analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol," IEEE Trans.parallel and distributed systems,vol 13, no 12, pp.1290-1302,Dec 2002.

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

[7] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Net-works,"Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

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

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security andPerformance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor NetworksUsing Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.

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

[12] G. Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing andComm. Workshops (PerCom), pp. 146-150, 2005.

[13] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[14] A. Shamir, "Identity-Based Cryptosystems and SignatureSchemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.

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

[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Frame-work for Wireless Sensor Networks Using

[17] Identity-Based Signa-tures," Proc. IEEE Int'l Conf.computer and information technology(CIT),pp 880-889.20

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

[19] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[20] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-LineDigital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275 1990.

[21] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. InformationSecurity and Privacy, pp. 99-110, 2006.