ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st& 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Secure Multi-Hop Data Transmission Over Cluster Based Wireless Sensor Network

Sathishkumar.S, Anitha.A,Revathi.S

Dept of Computer & Communication Engineering , M.A.M College of Engineering, Tamilnadu, India.

Dept of Information&Technology, Engineering, M.A.M College of Engineering, Tamilnadu, India.

M.A.M College of Engineering, Tamilnadu, India.

Abstract- In Wireless Sensor Networks (WSNs), secure data transmission is the major problem. LEACH protocols are used in wireless sensor networks which cause orphan node problem based on Security and require high Energy Consumption. Clustering technique is an effective way to enhance the system performance of wireless sensor networks. To address this problem Propose Secure and Efficient data Transmission (SET) protocols for Cluster Based Wireless Sensor Networks (CWSNs), called SET-IBS (Identity-Based digital Signature) scheme and SET-IBOOS (Identity-Based Online/Offline digital Signature) scheme. In the SET-IBS scheme, provide remedy for the cryptography problem in the pairing domain and used in Base Station of the Networks for security purpose. SET-IBOOS scheme is reduced to computational overhead for the protocol security and provide energy consumption for nodes. The SET protocol implements for one way hash function that enhances the security and also provide random key generation algorithm. The SET-IBS and SET-IBOOS protocols are used to provide the secure communication by using ID-Based Signature against attacks in the networks. These two schemes provide security and energy consumption for the Cluster based wireless sensor network.

Keywords– Cluster based Wireless Sensor Network, LEACH,SET-IBS, SET-IBOOS, ID based Digital Signature.

I.INTRODUCTION

A.WIRELESS SENSOR NETWORK

Sensor Networks are autonomous, self-organizing systems consisting of a multitude of small, inexpensive, battery-powered devices deployed densities in the deployment area. Sensor nodes systematically gather information from the environment and transmit the collected information to the sink or base station. In contrast to traditional wireless devices, sensor nodes are characterized by severe power, memory and computational constraints. In contrast to ad hoc network nodes, sensor network nodes are less mobile, are deployed in larger numbers and are in general, more limited in Capabilities [1]. Sensor networks are mainly used for gathering environmental information like temperature, pressure, humidity, and acoustic data. A wide range of real-world applications use sensor networksnamely habitat monitoring, structural monitoring, surveillance, disaster management, inventory management, target tracking, intruder detectionetc. The sensor node is usually scattered in a sensor field each of the scattered sensor nodes has the capabilities to collect data and route data back to the end user by a multi hop infrastructures through the sink. The sink may communicate with the internet to send data to the user.

B. CLUSTERING IN SENSOR NETWORKS

The sensor nodes are now deployed in large numbers and they are very affordable. The goal of a sensor network is to collect data from all the nodes and send the aggregated data to the base-station[2]. An obvious solution to this problem is clustering. The clustering protocols are used to minimize inter nodal communication in the network. The Clustering is to alternate active and sleep times and to use different levels of inter and intra cluster transmissions to conserve energy. The energy required to transmit a packet over a distance d is larger for a greater value of d. communicating with neighbors is less expensive than communicating with nodes that are situated at a greater distance. If the nodes communicate with the neighbors within a cluster only, the communications will be less expensive.

Clustering protocols gather data from all the nodes to conserving energy. It is claimed that clustering approaches are superior to non-clustering approaches in sensor network scenarios. Clustering approaches always outperform non-clustering approaches when there is a high degree of in-cluster data aggregation. The under low levels of in-cluster data aggregation, non-clustered approaches perform better. The clustering in the Network all the nodes are efficiently divided into disjoint subsets and within each such subset a header is elected. The header communicates with other clusters or the base-station.

C. AGGREGATION IN WSN

Aggregation techniques are used to decline the amount of data broadcast interior a WSN and therefore conserves electric battery power. As measurements are noted by all individual sensors, they need to be assembled and processed to make data of the entire WSN, such as mean and/or variance of the temperature or humidity inside a locality. One natural approach is for sensors to send their standards to certain exceptional nodes, i.e., aggregators. Each aggregator then condenses the data prior to dispatching it on. During periods of bandwidth and, aggregation, energy utilization is beneficial as long as the aggregation process is not too CPU-intensive.

The aggregators can either be outstanding (more powerful) nodes or usual sensors nodes. To assume that all nodes are potential aggregators and that data gets aggregated as they propagate to the go under [3]. In this setting, sensors have very restricted capabilities and aggregation should be easy and not engage any expensive or convoluted computations. It would need only a couple of easy arithmetic procedures, such as supplements or multiplications.

D. SECURITY IN SENSOR NETWORKS

Security in sensor networks is an emerging research area. As the technology becomes more mature, security concerns for sensor networks is becoming a key concern. Sensor networks are vulnerable to many attacks in the Networks. The main constraint is the limitation of resources and the small amount of energy that can be spared for implementing security protocols[4]. The Public key schemes and Diffie-Hellman scheme cannot be implemented in sensor networks. The key is used to provide security schemes that will provide data confidentiality, integrity and authentication. Sensor nodes typically use unprotected hardware and no physical shield that would stop access to the sensor's memory, processing, sensing and communication components. Thus, sensor networks are very weak to attack and security is very important.

The Trusted Platform Module is a secure crypto processor that can store cryptographic keys that protect information and the general name of the implementation of that specification. It offers facilities for the secure generation of cryptographic keys [5].Software can use a Trusted Platform Module to authenticate hardware devices in the network. TPM chip has a unique and secret RSA key burned in as it is produced, it is adept of accomplishing authentication.

E. IDENTITY-BASED SIGNATURES

Digital signatures are the most basic primitives in cryptography, providing the authentication, integrity, and non-repudiation. In their most basic form, each user in the system generates its own key pair consisting of a public key and a corresponding secret key, and the user is assumed to be uniquely identified by the public key. The users are generally not identified by randomly generated keys, by identities like the names or email addresses.To map public keys, identities called public-key infrastructure (PKI) needs to be set up, for involving a hierarchy of trusted certification authorities (CAs) that can certify the public keys as belong to the certain user.

In the identity-based setting, the public key of a user is identity, simplifying the PKI requirements. The corresponding secret key is issued by a trusted key generation center (KGC), derives it from a master secret that only the KGC to verify the identity of the user [6]. This eliminates some of the costs that associated to PKIs and certificates.

F. GROUP SIGNATURE SCHEME

A Group Signature scheme is a procedure for permitting a member of a group to anonymously signal a message on behalf of the group [7]. The group signature scheme could be used by an employee of a large company where it is adequate for a verifier to understand a message was signed by an employee, but not which particular employee sign it.

Group Signatures can be used to hide organizational structure, example when a business or a government agent issues a signed declaration. Group signatures can also be integrated with an electronic cash system whereby some banks can securely circulate anonymous and untraceable e-cash [8]. The group property can offer a further advantage of hiding the identity of the cash-issuing bank.

Essential to a group signature scheme is a group manager, who is in charge of adding group members and has the proficiency to reveal the initial signer in the happening of arguments. In some schemes the responsibilities of adding constituents and revoking signature anonymity are divided and granted to a membership manger and revocation supervisor respectively.

II. RELATED WORKS

WSNs generally established with the aimed at locality to supervise or sense the environment and depending upon the submission sensor node convey the data to the Base Station. The data intermediate nodes communicate simultaneously, choose an appropriate routing path and convey facts and figures towards the base position. Routing to selection counts on the routing protocol of the networks. Base stations should obtain

unaffected and new data. To fulfill this requirement, routing protocol should be energy-efficient and secure.

Hierarchical or cluster groundwork routing protocol for WSNs is the most energy-efficient among other routing protocols [9]. To investigate and compare secure hierarchical routing protocols founded on various criteria. Hierarchical routing is an effective way to reduce the total power consumption of the network. Data aggregation and processing in the CH is decreasing the total number of dispatched notes to the BS. The goal of developing a hierarchical routing protocol is to minimize the mesh traffic towards the base position. The security issue in a Hierarchical routing protocol has not been given much attention, since most of the routing protocol in WSNs has not been evolved with security. Many hierarchical routing protocols have been developed for power efficiency is the major goal.

The wireless sensor mesh (WSN) is a network scheme comprising spatially circulated devices using wireless sensor nodes to monitor the physical or biological situation, such as sound, warmth, and movement. In a WSN, the one-by-one nodes are adept of feeling their environments, processing the facts and data in the local area, and sending data to one or more collection points through a wireless connection. Sensor nodes are severely constrained by the energy from the batteries, which limits the lifetime and value of the mesh. Therefore, it is vital for WSNs to maximize nodes lifetimes, reduce bandwidth utilization by utilizing localized collaboration amidst sensor nodes [9]. Many sensor schemes are deployed in irregular and often adversarial physical environments, such as battlefields and military domains with trustless enclosures. This security is vastly demanded in numerous functional WSNs.

Focus on efficient, secure communications is a secure routing protocol using ID-based digital signature for cluster-based WSNs. In the proposed protocol, CHs are selected autonomously and communicate with the base station (BS) directly, where leaf sensor nodes join a cluster depending on the strength of the transmission signal. The secure routing protocol is based on the ID-based cryptography, in which users' public keys are their ID information, and users can obtain the corresponding private keys without auxiliary data transmission [10]. The secure protocol is efficient in communication. It suffers from high-computation cost for pairing. To analyze the positive and negative aspects of the proposed routing protocol quantitatively in calculations and simulations, with respect to both computational and communication cost.

Introduce an innovative kind of cryptographic scheme, which enables any two of users to transmit securely and to verify each other's signatures without exchanging private or public keys, key directories, and without using the services of a third party[10]. The design supposes the reality of trusted key generation centers.

The data embedded in this card enables the client to signal and encrypt the messages it sends and to decrypt and verify the messages are then obtains in a completely independent way, despite of the identity of the other party. Previously handed out cards do not have to be updated when new users join the network, and the diverse centers do not have to coordinate the interactivities or even to keep a client list. The centers can be shut after all the cards are handed out, and the network can extend to function in an absolutely decentralized way for an indefinite period.

The design is perfect for groups of users such as the executives of a multinational business or the branches of a large bank, since the head office of the corporation can assist as a key lifetime center that every person trusts. The design continues functional even on a nationwide scale with hundreds of key lifetime centers and millions of users, and it can be the cornerstone for a new kind of personal identification card with which every person can all mechanically sign checks, credit cards lips , legal document, and electrical devices mail.

III. CLUSTER BASED WIRELESS SENSOR NETWORK

The proposed architecture CWSN consisting of a fixed base station (BS) and a large number of wireless sensor nodes, are homogeneous in functionalities and capabilities. The BS is always reliable. The BS is a trusted authority (TA) [10]. Meanwhile, the sensor nodes may be compromised by the attackers, the data transmission may be interrupted from attacks on the wireless channel. CWSN, sensor nodes are grouped into clusters and each cluster has a cluster-head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy.

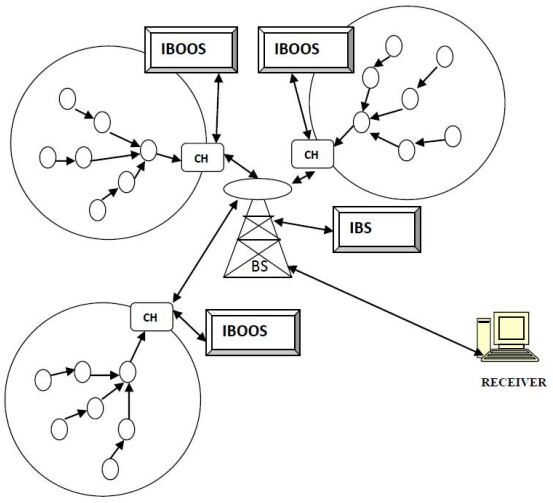

Fig.1Architecture of Secure Cluster Based WSN

The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, all sensor nodes and the BS are time synchronized with symmetric channels, nodes are deployed randomly, and the energy is constrained.

In CWSNs, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate

node (e.g., a CH) aggregates data and sends it to the BS is preferred, then the method that each sensor node directly sends data to the BS.

A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the TDMA (time division multiple access) control used for data transmission [11]. Implement, the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWSNs above.

IV. SECURITY VULNERABILITIES AND PROTOCOL OBJECTIVES

The data transmission protocols for WSNs, including cluster based protocols (LEACH-like protocols), are weak to a number of security attacks. 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 the CH, a sinkhole and selective forwarding attacks are provoked, thus disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the WSN, e.g., pretend as a leaf node sending bogus information towards the CHs [12]. But, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs. 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 in LEACH-like protocols reduce the risks of being attacked.

The goal of the proposed secure data transmission for CWSNs is to guarantee a secure and efficient data transmission to leaf nodes and CHs, and transmitted CHs and the BS. In existing secure transmission protocols for CWSNs is apply the symmetric key management for security, node suffers from the orphan node problem. Implement, to aim to solve the orphan node problem by using the ID-based crypto-system that guarantees security requirements [7], and propose SET-IBS by using the IBS scheme [13]. SET-IBOOS [14] is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

A.TheSET-IBS protocol operation

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

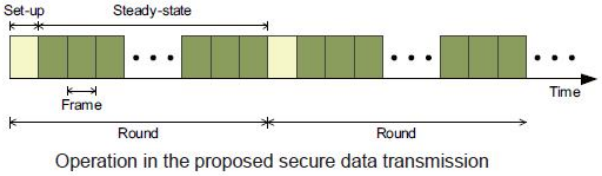

Fig.2 Operation of SET-IBS protocol

The operation of SET-IBS is divided by rounds. Each round includes a setup phase of constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS [15],[16]. In each round, the timeline is divided into consecutive time slots by the TDMA (time division multiple access) control.

Sensor nodes transmit the sensed data to the CHs in each frame of the steady state phase [17]. The fair energy consumption, nodes are randomly selected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission in the network, with the highest received signal strength of CHs. To elect CHs in a new round, each sensor node provides a random number and compares with the threshold value [18],[19]. The value is less than the value of the threshold value in the network. 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.

B.THE PROPOSED SET-IBOOS PROTOCOL OPERATION

To present the Secure and Efficient data Transmission (SET) protocol for CWSNs by using SET-IBOOS. 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 SETIBS, has a protocol initialization prior to the network deployment and operates in rounds during communication. To first introduce the protocol initialization, describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

C. PROTOCOL INITIALIZATION

In order to reduce the computation and storage costs of signature signing processing in the IBS scheme, to improve SET-IBS by introducing IBOOS for security in SET-IBOOS. The operation of the protocol initialization in SET-IBOOS is similartothe SET-IBS.The operations of key pre-distribution are revised for IBOOS.

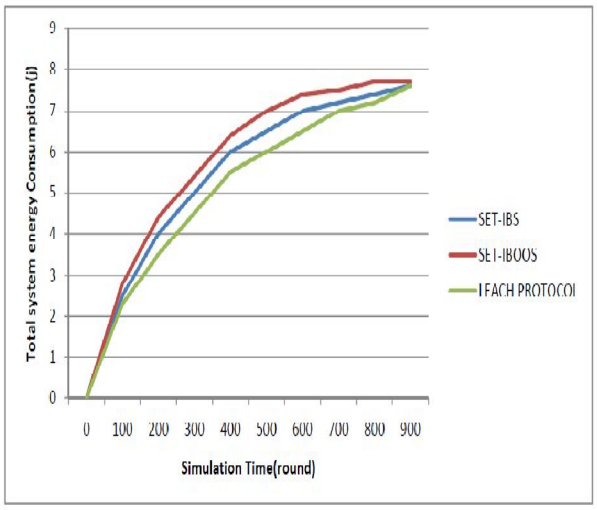

Fig. 3 Comparison of Energy Consumption in Different Protocols

V. SECURITY ANALYSIS

A. PASSIVE ATTACK ON WIRELESS CHANNEL

Passive attackers are able to perform eavesdropping at any level of the network, or even the whole communication of the network. Thus, they can undertake traffic analysis or statistical analysis based on the monitored or eavesdropped messages.

B. ACTIVE ATTACK ON WIRELESS CHANNEL

Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. The attackers can forge, reply and modify messages. Especially in WSNs, various types of active attacks can be triggered by attackers, such as bogus and replayed routing information attack, sinkhole and wormhole attack [21], selective forwarding attack, HELLO flood attack, and Sybil attack.

C.NODE COMPROMISING ATTACK

Node compromising Attackers are the most powerful adversaries against the proposed protocols as we considered. The attackers can physically compromise sensor nodes, by which they can access the secret information stored in the compromised nodes, e.g., the security keys. The attackers also can change the inner state and behavior of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

D. KEY MANAGEMENT FOR SECURITY

The SET-IBOOS private pairing parameters are preloaded in the sensor nodes during the protocol initialization [11]. The IBOOS scheme consists of following four operations, extraction, offline signing, online signing and verification.

Extraction: Before the signature process, it first extracts Private keys from the master secret key *x* and its identity *ID*.

Offline signing: Generates the offline signaturewith the time-stamp of its time slotfor transmission, and store knowledge for signing online signature when it sends the message. This offline signature can be done by the sensor node itself or by the trustful third party, e.g., the BS or the CH.

Online signing: At this stage, node *Ai* computes the online Signaturebased on the encrypted dataand the offline signature.

Verification: It checks the current time-stamp *ti*for freshness. Then, if the time-stamp is correct, the sensor node further computes

VI. SECURE MULTI-HOP DATA TRANSMISSION

A. CLUSTER

In this component it constructs CWSN. In which sensor nodes are grouped into clusters, and each cluster has a cluster-head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save the energy. The CHs performed data fusion, and transmit data to the BS directly with comparatively high energy. In addition, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are randomly distributed, and the energy is constrained.

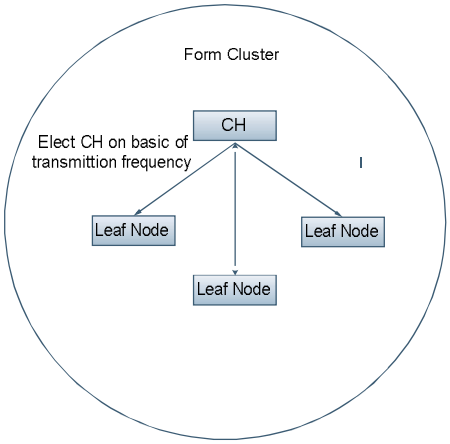

Fig.4Cluster Model

B. BASE STATION

Thefixed base station used for cluster-base wireless sensor networks. A Base Station is responsible to give authority (certificate and key) for every node in the cluster.

C. SET-IBS

SET-IBS (Identity-Based digital Signature) scheme the base station generates a master key and public parameter for private key generator and gives that all to sensor node in the cluster. Then sensor node generates a private key use a private string after that send messages along with a timestamp and signature. Signature is generated by signing key. In receiver side message

accepted if verification of the signature is valid otherwise rejected.

TABLE 1:OPERATION SIN SET-IBOOS

Setup phase			
STEP 1	BS => G_s	<ID_{bs}, T_s,nonce>	The BS broadcasts its information to all nodes.
STEP 2	CH => G_s	< ID_i, T_s, adv,σ_i,c_i>	The elected CHs broadcast their information.
STEP3	L_i→ CH_i	<ID_i, ID_j, T_s, join, σ_i, c_i>	A leaf node joins a cluster of CH
STEP4	CH_i => G_s	< ID_i, T_s, sched(...,ID_j|T_j,...),σ_i,c_i >	A CH i broadcasts the schedule message to its member.
Steady-state phase			
STEP 5	L_i→ CH_i	<ID_i, ID_j, T_j, C, σ_j, c_j>	A leaf node j transmits the sensed data to its CH i.
STEP6	CH_i → BS	:<ID_{bs},ID_i, T_s, F, σ_i, c_i>	A CH i transmits the aggregated data to the BS.

Notation

=>, →	Broadcast and Unicast transmission.
L_j,CH_i,G_s	A leaf node, a cluster head, and the set of sensor nodes in the network
T_s, t_i	Time-stamps denoting the time slot for transmission in setup and steady-state phases.
ID_i, ID_{bs}	The ID of a sensor node i or the BS.
C, F	Encrypted sensed data and aggregated data
adv, join, sched	Message string types which denote the advertisement, join request, and schedule messages.
<σ_i,c_i>	The ID based digital signature concatenated with data from node i

D. SET-IBOOS

The SET-IBOOS (Identity-Based Online/Offline digital Signature) scheme in this the base station generates a master key and public parameter for private key generator and give that all sensor nodes in the cluster. Then sensor node generates a private key use a private string after that a cluster head use that sting id and time stamp cluster head generate offline signature send it to the leaf node [13]. And then use the private of sensor nodes, offline signature and message every sensor node generates online signature .In receiver side cluster head accepted message if the signature is online otherwise rejected.

TABLE 2:OPERATIONS IN SET-IBOOS

Setup phase			
STEP 1	BS => G_s	<ID_{bs}, T_s,nonce>	The BS broadcasts its information to all nodes.
STEP 2	CH => G_s	< ID_i, T_s, adv,σ_i,z_i>	The elected CHs broadcast their information.
STEP3	L_i→ CH_i	<ID_i, ID_j, T_s, join, σ_i, z_i>	A leaf node joins a cluster of CH
STEP4	CH_i => G_s	< ID_i, T_s, sched(...,ID_j|T_j,...),σ_i,z_i >	A CH i broadcasts the schedule message to its member.
Steady-state phase			
STEP 5	L_i→ CH_i	<ID_i, ID_j, T_j, C, σ_j, z_j>	A leaf node j transmits the sensed data to its CH i.
STEP6	CH_i → BS	<ID_{bs} ,ID_i, T_s, F, σ_i, z_i>	A CH i transmits the aggregated data to the BS.

Notation

=>, →	Broadcast and Unicast transmission.
L_j,CH_i,G_s	A leaf node, a cluster head, and the set of sensor nodes in the network
T_s, t_i	Time-stamps denoting the time slot for transmission in setup and steady-state phases.
ID_i, ID_{bs}	The ID of a sensor node i or the BS.
C, F	Encrypted sensed data and aggregated data
adv, join, sched	Message string types which denote the advertisement, join request, and schedule messages.
<σ_i,z_i>	The ID based digital signature concatenated with data from node i
$\sqrt{\sigma_i}$	The offline signature of node i concatenated with data.

ACKNOWLEDGMENT

I would like to thank Ms.A.Anitha and Ms.S.Revathifor helpful discussions about this work.

VI.CONCLUSION

The Security and Data Transmission in Cluster founded Wireless Sensor Networks. The deficiency of the symmetric key administration for protects transmission. The Offered SET-IBS and SET-IBOOS to protect and effective transmission protocols, respectively for Cluster founded Wireless Sensor systems. Feasibility of the SET-IBS and SET-IBOOS makes security obligations and investigation against Routing Attacks. SET-IBS and SET-IBOOS are produced in connection and applying the ID-based crypto-system, which accomplishes security obligations in CWSNs, as well as clarified the orphan node difficulty in the protected transmission protocols with the symmetric key management, using SET-IBOOS and SET-IBS are less auxiliary security overhead is preferential for secure data transmission. Future advancement shows the energy consumption for every node in the network with the transfer data in secure and efficient for CWSNs.

REFERENCES

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

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

[3] C.Castelluccia, E. Mykletun, and G. Tsudik, "*Efficient aggregation of encrypted data in wireless sensor networks,"* in *Proc. MobiQuitous*, 2005.

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

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

[6] H. Lu, J. Li, and H. Kameda, "*A Secure Routing Protocol for Cluster-Based WSNs Using ID-Based Digital Signature,"* in *Proc. IEEE GLOBECOM*, 2010.

[7] A.Shamir, "*Identity-Based Cryptosystems and Signature Schemes*," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985.

[8] 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.

[9] S.Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in *Proc. ICCCS*, 2011.

[10] J.Liu and J. Zhou, *"An Efficient Identity-Based Online/Offline Encryption Scheme,"* in *Lect. Notes. Comput. Sc. - Appl. Crypto. Netw. Secur.*, 2009.

[11] C Karlof and D. Wagner, *"Secure routing in wireless sensor networks: attacks and countermeasures,"Ad Hoc Networks*, vol. 1, no. 2-3, 2003.

[12] S.Xu, Y. Mu, and W. Susilo, *"Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security,"* in *Lect. Notes. Comput. Sc. - Inf. Secur.*

[13] Boneh and M. Franklin, *"Identity-Based Encryption from the Weil Pairing,"* in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001.

[14] S. Even, O. Goldreich, and S. Micali, *"On-Line/Off-Line Digital Signatures,"* in*Lect. Notes. Comput. Sc. - CRYPTO*, 1990.

[15] C.-K. Chu, J. K. Liu, J. Zhou *et al.*, *"Practical ID-based encryption for wireless sensor network,"* in *Proc. ACM ASIACCS*, 2010.

[16] F. Hess, "*Efficient Identity Based Signature Schemes Based on Pairings,"* in *Lect. Notes. Comput. Sc. - SAC*, 2003.

[17] J. J. Rotman, *An Introduction to the Theory of Groups*. Springer-Verlag; 4th edition, 1994.

[18] K. S. McCurley, *"The discrete Logarithm Problem,"* in *Proc. Symp. Appl. Math.,Prog. Com. Sc.*, 1990, vol. 42.

[19] H. Lu, J. Li, and G. Wang, *"A Novel Energy Efficient Routing Algorithm forHierarchically Clustered Wireless Sensor Networks,"* in *Proc. FCST*, 2009.