Secure and Efficient Data Transmission in Wireless Sensor Network Using SET Protocols

[1] K.Shanmugam,[2]Dr.B.Vanathi, [3]Azhagu Raja R ,[4]R.A.Priyanka,[5]Shiyanashiny
[1]Assistant Professor,[2] Professor,[3] PG Scholar, [4,5]UG scholar
[1,2,4,5]Dept of CSE,Valliammai Engineering College,Chennai,Tamilnadu
[3] Dept of CSE, SMK Fomra Institute of Technology, Chennai, India.

Abstract— Wireless sensor networks (WSNs) are increasingly used in many applications, such as volcano and fire monitoring, urban sensing, and perimeter surveillance. Today wireless sensor networks are broadly used in environmental control, surveillance tasks, monitoring, tracking and controlling etc. On the top of all this the wireless sensor networks need very secure communication in wake of them being in open field and being based on broadcasting technology. Different protocols or algorithms are designed to improve the energy of wireless sensor network. In this paper we discus about different data aggregation techniques to improve energy efficiency in WSN. In a large WSN, in-network data aggregation (i.e., combining partial results at intermediate nodes during message routing) significantly reduces the amount of communication overhead and energy consumption. Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Project show the feasibility of the SET-IBS and SET-DTA 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.

Keywords— **Wireless Sensor Networks, Secure and Efficient Data Transmission, Identity Based Digital Signature, Cluster Based Wireless Sensor Networks, Decentralized Timestamp Authentication.**

I.INTRODUCTION

Over the Last Decade Wireless Sensor Networks consist of numerous autonomous sensor nodes devices are spatially distributed to sense and monitor various changes of the environment surrounding us. Such devices are also capable to communicate in wireless sensor networks and that can also sense, monitor, transmit, receive or process numerous data like pressure, temperature, sound, motion, humidity etc. The following section discussed about various sensor deployment environments and previously deployed schemes in the proposed domain.

The data transmission in WSNs can be done in two ways: (i) centralized (ii) decentralized. Centralized means such data processing and transfer can be carried out through or via the medium of a base station in WSNs [3]. Whereas, in case of distributed or clustered wireless sensor environments, every cluster has obtained a high-configuration node called a cluster-head (CH). A sensor node of one cluster can only communicate with the other cluster‘s sensor node by taking the permission of the respective cluster. It is the function of cluster-head to aggregate all the data sent by sensor nodes present in its vicinity. Eventually, cluster-heads sent all the data to the master storage known as base station (BS).

The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In a cluster-based WSN (CWSN), it is a better approach to keep a powerful base station which can compute or store large amount of data if required. The reason behind this approach is sensor nodes present in the respective clusters are equipped with limited energy and memory requirements and once they are deployed these nodes also need to process data of their neighboring nodes as well. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the cluster-based architecture in the real world is rather complicated [10]. After rigorous analysis of previously proposed protocols like LEACH, Sec-LEACH [2], RLEACH [8], GS-LEACH, we have reached to the conclusion that all these schemes can easily address routing issues present in the WSNs but they have limited scope to provide security against high-level security attacks is still an opportunity to carry-out a detailed research and implement a cost effective efficient solution. From these results, we have also found that most of the security attacks can be protected or avoided by time-stamp based authentication schemes [11]. In this paper, we have also addressed an issue of orphan node problem by using asymmetric key mechanism rather than symmetric key mechanism for CWSNs. Mainly security of CWSNs can be divided into three categories: [i] base station security [ii] cluster-based security [iii] sensor node security. To address all these security issues, we have divided the proposed security protocol SETDTA into two processes: a) authentication process b) session establishment process.

II.RELATED WORK

Several researchers have studied problems related to data aggregation in WSNs.

A. Data Aggregation in a Trusted Environment

The Tiny Aggregation Service (TAG) to compute aggregates,such as Count and Average, using tree-based aggregation algorithms were proposed in [3]. Similar algorithms to compute aggregates were proposed in [8]. Moreover, tree based aggregation algorithms to compute an order-statistic (i.e., quantile) have been proposed in [9].To address the communication loss problem in tree-based algorithms an aggregation framework called *synopsis diffusion* is designed in [9], which computes Count and Sum

using a ring topology. Very similar algorithms are independently proposed in [3]. These works use duplicate-insensitive algorithms for computing aggregates based on [9]'s algorithm for counting distinct elements in a multi-set.

B. Secure Aggregation Techniques

Several secure aggregation algorithms have been proposed assuming that the BS is the only aggregator node in the network [10]–[12]. These works did not consider in-network aggregation. Only recently, the research community has been paying attention to the security issues of hierarchical aggregation.

1. Tree Based Data Aggregation

Tree-based data aggregation approach builds an aggregation tree. This tree is a minimum spanning tree, sink node as root node and leaves consider as source node. In this technique data is transferred from leaves node to sink node and aggregation is done by parent nodes.
Ex. TAG (Tiny AGgregation) performs the data aggregation process with the help of queries process. It provides service for aggregation in distributed, low-power, wireless environments. [3]

2. Centralized Data Aggregation

Data is gathering at centre node in centralized data aggregation technique. For this process it takes the help of shortest path using a multi-hop wireless protocol. The sensor nodes send the data packets to a centre node, which is the powerful node. The leader aggregates the data which can be queried. Each intermediate node has to send the data packets addressed to leader from the child nodes. So a large number of messages have to be transmitted for a query in the best case equal to the sum of external path lengths for each node. Ex. DD, SPIN.

C. Secure Data Transmission Techniques

The data transmission in WSNs can be done in two ways: (i) centralized (ii) decentralized. Centralized means such data processing and transfer can be carried out through or via the medium of a base station in WSNs [10]. Whereas, in case of distributed or clustered wireless sensor environments, every cluster has obtained a high -configuration node called a cluster-head (CH). A sensor node of one cluster can only communicate with the other cluster‘s sensor node by taking the permission of the respective cluster. It is the function of cluster-head to aggregate all the data sent by sensor nodes present in its vicinity. Eventually, cluster-heads sent all the data to the master storage known as base station (BS). The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs [15]. In a cluster-based WSN (CWSN), it is a better approach to keep a powerful base station which can compute or store large amount of data if required. The reason behind this approach is sensor nodes present in the respective clusters are equipped with limited energy and memory requirements and once they are deployed these nodes also need to process data of their neighbouring nodes as well. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the cluster-based architecture in the real world is rather complicated . After rigorous analysis of previously proposed protocols like LEACH, Sec-LEACH, RLEACH, GS -LEACH, we have reached to the conclusion that all these schemes can easily address routing issues present in the WSNs but they have limited scope to provide security against high-level security attacks is still an opportunity to carry-out a detailed research and implement a costeffective efficient solution. From these results, we have also found that most of the security attacks can be protected or avoided by time-stamp based authentication schemes [3].

III. SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

This section presents the network architecture, security vulnerabilities, and protocol objectives.

A. Network Architecture

Consider a CWSN consisting of a fixed BS and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume

that the BS is always reliable, i.e., the BS is a trusted authority (TA).Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are grouped into clusters, and each cluster has a 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. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their 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 than the method that each sensor node directly sends data to the BS [5], [8]. A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the time-division multiple access (TDMA) control used for data transmission. In this paper, the proposed SET-IBS and SET-DTA are both designed for the same scenarios of CWSNs above.

B. Security Vulnerabilities and Protocol Objectives

The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [11], [15]. 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 [2]. 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 [11], [12], [15], 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-DTA is proposed to reduce the computational overhead in SET-IBS with the DTA scheme.

IV. SECURE DATA TRANSMISSION WITH HIERARCHICAL CLUSTERING

In large-scale CWSNs, 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. The solutions to this extension could be achieved by applying the following two routing models:

1.The multihop planar model

A CH node transmits data to the BS by forwarding its data to its neighbour nodes, in turn the data are sent to the BS. We have proposed an energy -efficient routing algorithm for hierarchically clustered WSNs in [8], and it is suitable for the proposed secure data transmission Protocols.The cluster-based hierarchical method. 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, for example, [9].

2. Security Analysis

To evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs that threaten the proposed protocols, and the cases when an adversary (attacker) exists in the network. Afterwards, we detail the solutions and countermeasures of the proposed protocols, against various adversaries and attacks.

2.1 Attack Models

In this paper, we group attack models into three categories according to their attacking means as follows, and study how these attacks may be applied to affect the proposed protocols:

Passive attack on wireless channel: Passive attackers are able to perform eavesdropping at any point 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.

Active attack on wireless channel: Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, 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, selective forwarding attack,

HELLO flood attack, and Sybil attack .

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, for example, 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.

V.PROTOCOL EVALUATION

1. IBS AND DTA FOR CWSNS

In this section, we introduce the IBS scheme and DTA 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 [7] at first. To further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional Identity Signature scheme for CWSNs, based on [2].

1.1 Pairing for IBS

For self-contained, we briefly review the characteristics of pairing.Boneh and Franklin [13] introuduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically,

2.SET-DTA Scheme for CWSNs

In this section, we introduce the new version of IBS scheme by using new version of El-gamal digital signature authentication scheme for the random numbers. Here, we have modified the conventional IBS scheme and used asymmetric encryption scheme to mitigate the problem of orphan node in CWSNs. In order to reduce the communication and computational overhead during the digital signature signing and verification process, we have introduced novel timestamp based solution. The digital signature scheme which has been used in the implementation of this protocol uses the public key cryptography for encryption and signature verification. For each user, there is a For each user there is a secret key x and corresponding public keys are α, β, p where [10]:

$$\beta = \alpha^x mod\, p \ldots\ldots\ldots\ldots\ldots\ldots.(i)$$

Here, α, β and p are publics keys which are kept public and x will be kept secret.

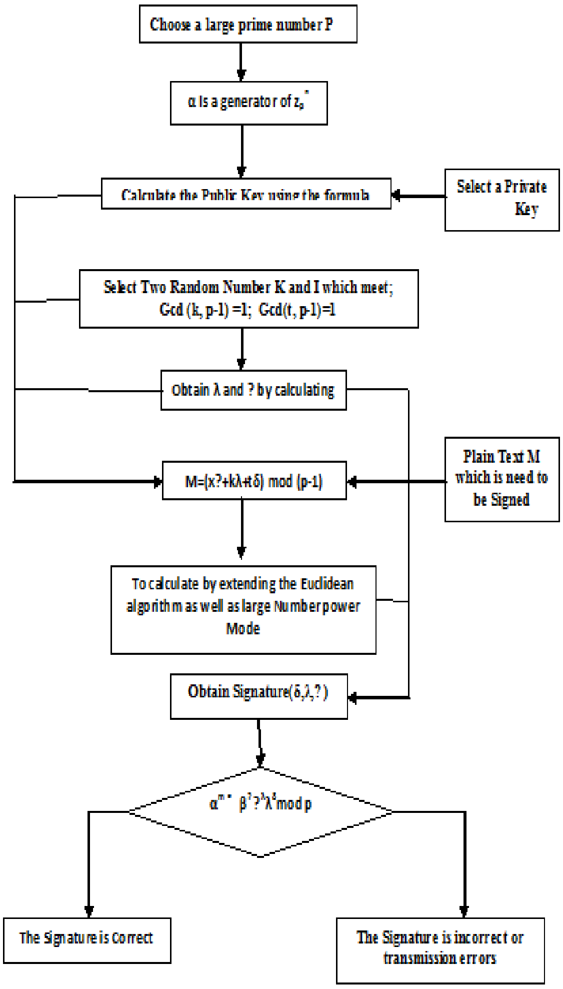
$$\alpha^x = \beta \; mod \; p \ldots\ldots\ldots\ldots\ldots\ldots.(ii)$$

Here, p is a large prime number and choose a random number k such that 0<k<p-1 and gcd (k, p-1) = 1.

$$\alpha^x = \beta \; mod \; p \ldots\ldots\ldots\ldots\ldots\ldots.(ii)$$

$$\gamma=\alpha^x \; mod \; p \ldots\ldots\ldots\ldots\ldots\ldots\ldots.(iii)$$

Detailed process of digital signature generation process is shown in the following figure


Choose a large prime number P
α Is a generator of z_p^*
Calculate the Public Key using the formula
Select a Private Key
Select Two Random Number K and I which meet; Gcd (k, p-1) =1; Gcd(t, p-1)=1
Obtain λ and ? by calculating
M=(x?+kλ+tδ) mod (p-1)
Plain Text M which is need to be Signed
To calculate by extending the Euclidean algorithm as well as large Number power Mode
Obtain Signature(δ,λ,?)
α^{m} β? ?λ mod p
The Signature is Correct
The Signature is incorrect or transmission errors

3 .The Proposed SET-DTA Protocol

In this paper, we propose a novel protocol called
—Secure and efficient transmission- Decentralized Timestamp based Approachǁ for CWSNs. The proposed SET-DTA consists of the following operations, specifically, setup at the BS, key management and signature signing of the transmitting sensor nodes and verification of the receiving sensor nodes. In this proposed scheme, we assume that, all the sensor nodes have knowledge of the current timestamp tc and the sending time-stamp ts.

3.1 Protocol initialization

The proposed SET-DTA scheme has following procedural steps:
3.1.1 System Initial Setup Procedure The step by step description of the proposed SET-DTA scheme is as follows:

a. First of all, BS registers all the valid sensor nodes and also generates private key for all the register nodes, International Journal of Advanced Engineering Applications, Vol.7, Iss.2, pp.60-73 (2014)

b. In addition, Base Station also registers all the verified users and created their private keys.

c. When a sensor node A registers with the base station, it keeps the record of sensor nodes by storing the identity of sensor node with the sending time-stamp TS.

d. To provide the additional security against various attacks the BS sends registration information encrypted with the hash function H like (H (SIDA), TS).

e. After receiving the broadcasted information from the Base Station, all the sensor nodes present in the network will reply by ending their acknowledgements respectively. In addition,
if a sensor node will not receive any information, it won‘t send any ACK to the Base Station. To the all silent nodes, the base station immediately resends the message again. In this proposed scheme it is assumed that the Base Station will never store

generated secret keys of sensor nodes and users.

4. SET-DTA PROTOCOL EVALUATION

This section describes SET-DTA protocol characteristics and features, security analysis and various sensor-kit simulation results.

4.1 Protocol Characteristics and Features

In this section, we summarize the characteristics of the proposed SET-DTA protocol. Figure 1 and 2 shows the general procedure and steps of the proposed SET-DTA protocol. We have done rigorous practical and theoretical analysis of the proposed protocol to evaluate its performance. All the analysed characteristics are as follows.

4.1.1 Key Management

Standard cryptography techniques are used in this protocol to achieve secure data transmission, which consist of symmetric encryption, hash algorithm and RSA algorithm based security [13].

4.1.2 Authentication Procedure

Secure authentication procedure based on current and sending time-stamp has been followed to achieve strong authentication against high-level security attacks.

4.1.3 Communication Overhead

This protocol assures less communication overhead as all the required mechanisms like digital signatures, public and private keys are stored on the base station(s).

4.1.4 Computation Overhead

We have designed this protocol in such a way that it assures secure and efficient transmission between the sensor nodes and a base station(s).

4.1.5 Protection against Security attacks

This proposed scheme very much focused on providing a strong defence against high-level security attacks like node capture attack, cloning attack etc.

4.2 Security Analysis

To evaluate the security of the proposed protocol SET-CTA, we have analyzed various range of security attacks and the scenarios when a malicious node exists in the network and try to intercept the communication between the sensor nodes. In the remainder part, we have described how this proposed protocol can provide strong defence against various adversaries and attacks.

4.2.1 Node Compromising Attacks

Such attacks and attackers are considered as the most threaten adversaries. Such attackers can access the secret information stored in the compromised nodes, e.g., private or public keys, session keys, node identities etc.

4.2.2 Passive Attacks

Attacks like eaves dropping, traffic congestion can be initiated during anytime of the wireless network deployment. Such passive attackers can also monitor the network and can prepare themselves for carryingout future attacks .

4.2.3 Active Attacks/Real-time Attacks

Active attackers have greater ability than passive adversaries, which can tamper with the active wireless channels. Therefore, the attackers can forge, reply and modify messages. Nowadays in WSNs, attackers have started implementing numerous active attacks like bogus and replayed routing attacks, node-capture attack, cloning attack etc.

VI. CONCLUSION AND FUTURE WORK

This paper presents a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically the security issues of in-network aggregation algorithms to compute aggregates such as predicate Count and Sum. In particular, Secure and efficient data transmission in WSN using SET protocol showed the falsified sub-aggregate attack launched by a few compromised nodes can inject arbitrary amount of error in the base station's estimate of the aggregate. An attack-resilient computation algorithm which would guarantee the successful computation of the aggregate even in the presence of the attack. The proposed SET-IBS and SET-DTA protocols have better performance than existing secure protocols for CWSNs Which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission.

The Future work will focuses on developing new routing algorithms for routing the data from the source to the sink. This approach should confront with the difficulties of topology construction, data routing, loss tolerance by including several optimization techniques that further decrease message costs and improve tolerance to failure and loss. Later, I will simulating SEDT in WSN using SET protocol technique and compare it with some protocols to prove its efficiency.

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. Future researchers come up with smarter and more robust security mechanisms and make their network safer.

REFERENCES

[1] Leandro Villas, Azzedine Boukerche1, Heitor S. Ramos “DRINA: A Lightweight and Reliable Routing Approach for in-Network Aggregation in Wireless Sensor Networks” , IEEE 2013

[2] Erfan. Arbab, Vahe. Aghazarian, Alireza. Hedayati, and Nima. Ghazanfari Motlagh, “A LEACH-Based Clustering Algorithm for Optimizing Energy Consumption in Wireless Sensor Networks”, ICCSIT'2012

[3] Samuel Madden, Michael J. Franklin, and Joseph M. Hellerstein, “TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks”,OSDI, December, 2002.

[4] M. Liu, N. Patwari, and A. Terzis, “Scanning the issue,” *Proc. IEEE*, vol. 98, no. 11, pp. 1804–1807, Apr. 2010.

[5] T. Ko, J. Hyman, E. Graham, M. Hansen, S. Soatto, and D. Estrin, “Embedded imagers: Detecting, localizing, and recognizing objects and events in natural habitats,” *Proc. IEEE*, vol. 98, no. 11, pp. 1934–1946, Nov. 2010.

[6] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, “Environmental wireless sensor networks,” *Proc. IEEE*, vol. 98, no. 11,pp. 1903–1917, Nov. 2010.

[7] (2006). *James Reserve Microclimate and Video RemoteSensingO*nline.Available:http://research.cens.ucla.edu/ projects/2006/terrestrial/microclimate/defau%lt.htm

[8] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, “TAG: A tiny aggregation service for ad hoc sensor networks,” in *Proc. 5th USENIX Symp. Operating Syst. Des. Implement.*, 2002, pp. 1–3.

[9] J. Zhao, R. Govindan, and D. Estrin, “Computing aggregates for monitoring sensor networks,” in *Proc. 2nd Int. Workshop Sensor Netw.Protocols Appl.*, 2003, pp. 139–158.

[10]. L. Huang, J. Li, M. Guizani, ―Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks,‖ IEEE Trans. Parallel and Distri. Syst., 2012.

[11]. Modares, Hero; Salleh, Rosli; Moravejosharieh, Amirhossein;, "Overview of Security Issues in Wireless Sensor Networks," Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on , vol., no., pp.308-311, 20-22 Sept. 2011.

[12]. Xiaowang Guo; Jianyong Zhu; , "Research on security issues in Wireless Sensor Networks," Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on , vol.2, no.,pp.636639, 12-14 Aug. 2011.

[13]. HongShan Qu; Wen Liu; , "A robust key predistribution scheme for wireless sensor networks,"Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.634-637, 27-29 May 2011.

[14]. Wang Hai-Chun; Huang Tao; , "Design of Security Gateway Based on Chaotic Encryption,"Internet Technology and Applications (iTAP), 2011 International Conference on , vol., no., pp.1-4, 16-18 Aug.2011.

[15]. Burgner, D.E.; Wahsheh, L.A.; , "Security of Wireless Sensor Networks," Information Technology: New Generations (ITNG), 2011 Eighth International Conference on , vol., no., pp.315-320, 11-13 April 2011.