**Journal of Computer Science 9 (9): 1174-1180, 2013**
ISSN: 1549-3636
© 2013 Science Publications
doi:10.3844/jcssp.2013.1174.1180 Published Online 9 (9) 2013 (http://www.thescipub.com/jcs.toc)

# SECRET HANDSHAKE ISSUE AND VALIDATE AUTHORITY BASED AUTHENTICATION SYSTEM FOR WIRELESS SENSOR NETWORK

**[1]Kamalanaban Ethala, [2]R. Seshadri, [3]N.G. Renganathan and [4]M.S. Saravanan**

[1]Department of CSE, Sri Venkateswara University, Tirupathi, India and
Vel Tech University, Avadi, Chennai, India
[2]SVU Computer Center, Sri Venkateswara University, Tirupathi, India
[3]Vel Tech University, Avadi, Chennai, India
[4]Department of IT, Vel Tech University, Avadi, Chennai, India

Received 2013-07-04, Revised 2013-07-23; Accepted 2013-08-03

## ABSTRACT

Wireless Sensor Networks (WSN) are major research area in the past few decades. WSN is formed by collection of sensor nodes. Power source life and memory size limit the hardware sources and these will decide the lifesapn of sensor nodes in WSN. Therefore, many resources based research issues are evolved in WSN. This study focused security issue and proposed authentication system. As the sensor nodes are limited memory, the traditional authentication systems are uncomforted. Hence, secret handshake system using two authorities, namely Issue Authority and Validate Authority are proposed in this study. The proposed authentication system is called as, Secret Handshake Issue and Validate Authority (SHIVA). The proposed methodology is occupying lesser memory space and also reducing number of communication of sensor nodes for the authentication model. Therefore, the proposed methodology proved optimum for WSN.

**Keywords:** Wireless Sensor Network, Authentication, Secret Handshake, Issue Authority

## 1. INTRODUCTION

WSN become an ideal framework for monitoring the environment data through the collection of distributed collaborative sensor nodes. WSN consists of a large number of sensor nodes. These are distributed networks. These will not have a centralised system but provided with self powered by a battery and hence they are capable of doing computation equipped with a processor and a communication module. These WSN find applications in monitoring meterological data. These are also used in tracing targets in the battle field, border security. These networks are also employed in detecting forest fire, monitoring health, habitat. These data are immensely useful for the policy makers and hence these networks are absolutely essential.

The number of applications using WSN is growing rapidly over the years. Hence, protecting sensor nodes from malicious attacks becomes a challenging task and many of the WSN applications need secured data transfer. In the deployment of WSN security is an important aspect. This is a must in WSN networking which are to be unattended. The sensor nodes are limited resources and thus implementation of the security model is more critical in WSN, since sensor nodes must be provided with enough memory to retrieve the information stored in security keys (Xiaowang and Jianyong, 2011).

These problems are very common in WSN and these limitations lead to challengeable proposal in the variety of research issues for the past few years.

There are various protocols for encryption or decryption technologies in wired networks. Diffie

**Corresponding Author:** Kamalanaban Ethala, Department of CSE, Sri Venkateswara University, Tirupathi, India

Hellman protocol or RSA algorithm that are adopted in these kind of networks are not going to be useful since they are difficult in implementation stages in WSN. These traditional methodologies required large amounts of power dissipation and also involves various complicated problems related to key management and access control. It is seen from the literature that many encryption methods are not applicable from two anlges. (i) they do not have support schemes like the asymmetric encryption method. (ii) they do not have a trusted third party to manage users andkey registers In the method of application of these networks also it has drawbacks. In these the input messages have to be signed and enciphered and then only it should be sent via the network. This is not achieved in practice. Hence the efficiency is lost in these networks since security will be lost. This is because of third party intervention and the access to the information is gained by the third party.Hence the most important step, user authetication, which is a preventive measure against outside attack is lost in these procedures (El-Khatib, 2010). Therefore, sufficient resources are needed to implement the traditional encryption methods, in order to handle these various tasks. Hence this study proposes a user authentication mechanism to counter measure the attacks initiated by the intruders.

The potential attacks are classified into five categories:

- Jamming Attacks-this kind of attack occurs in the physical layer. This attack is injected to disturb sensor node communication and the transmission of messages
- Black-hole attacks-This kind of attack appears in the network and routing layer. The modus operandi in this type of attack is to create a black-hole. This node is a compromised node. This sends messages to its neighbouring nodes. This is done to transmit packets to destinations using minimal routing. The advantage of this method is to add or delete any message in the neighbouring nodes as they are stored in temporary buffer. Thus a black hole scenario is created for the transmission
- Power or Flooding attacks-this is another type of attack and this occurs in the transport layer. This leads to power failure in this layer. An attacker sends number of messages. By this process the system will try to establish a connection with a node and thus try to exhaust its power in the process
- De-synchronization attacks- This type of attaks also occurs in the transport layer. In this attack the attacker transmits some packets to forged packets. This will enable the connection between any two peer nodes. The attacker in addition to the messages also sends some numbers in various sequences. This type of attack is to create requests to the other nodes to send the last packet again. This is to create traffic jam till the power overload is created
- Capture attacks- This is another form of attack.It is very difficult to prevent thses type of attacks, if nodes are not tamper-proof and the environment is left unattended

Most of the aforementioned attacks can be eliminated using authentication mechanism. The Intrusion Detection System (IDS) is a known authentication mechanism. This mechanism can be operated in two ways. They are: (i) anomaly detection and (ii) misuse detection. The anomaly detection is able to identify new types of attack but it may raises false alarms in some environments. The misuse detection is unable to identify new types of attacks, but it has a high correct-detection rate for known types of attacks. The surveys on IDS are discussed in the next sections.

## 2. MATERIALS AND METHODS

In information systems, the intrusive activities carried out in the network are detected by an Intrusion Detection System (IDS). The IDS is a security layer protocol. This is a major line of defence for protecting network resources from illegal penetrations. In general, the intrusion detection requires extensive knowledge of security experts and algorithms. These may involve more computational costs. In order to reduce computational cost, many IDS are proposed to reduce this dependence (El-Khatib, 2010). Hence various data-mining and machine learning techniques have been deployed for intrusion detection.

The IDS have to work in a dynamically changing environments. This requiresforces continuous tuning of the intrusion detection model. This is to maintain sufficient performance. The manual tuning process required by current system depends on the system operators which have to work out the tuning solution in integrating it into the detection model. It is (Xiaowang and Jianyong, 2011) proposed an automatic tuning IDS (ATIDS). By this the system will automatically tune the detection model on-the-fly according to the feedback provided by the system operator when false predictions are encountered (Modares *et al*., 2011).

A common approach in intrusion detection models, specifically in anomaly detection models, is to use classifiers as detectors. In these best features have to be selected. The features are to ensure the performance, speed of learning. At the same time it must ensure accuracy and reliability. To have a good classifier the detector should be free from noise and thus it will have efficient and accurate in detecting network attacks. Still it will not detect 802.11 specfic attacks. These attacks are de- authenitication attacks. These attacks are also known as MAC layer DoS attacks. To overcome these El-Khatib (2010) proposed a hybrid model. This is to detect 802.11 specific intrusions.For this optimal set of features will be selected. By this model feature selection will be first made. Then k-means classifier will be used to select the optimal set of MAC layer feature. This procedure will not only reduce the learning time of the algorithm but it will improve the accuracy also. The handshake is the specific algorithm and this is used to distinquish the member and the attacker. For useful authentication protocol Secret Handshake sechemes are used and these are recent models. By this any user can communicate with another user of the same group and they can use the Secret handshake algorithm (Dong *et al*., 2011).

The SH scheme enables two members who belong to G to authenticate each other in a way that hides their affiliation from all others. The SH scheme was initiated by (Modares *et al*., 2011). In this model, a two-party SH is designed, by adapting the key agreement protocol, based on the bilinear Diffie-Hellman assumption.

Unlink ability is newly added research issue in the information system. This is ability to the extent to which handshake players cannot be linked. Since the member sends his ID in a handshake protocol, SH schemes in many security models un satisfy the unlink ability (Dong *et al*., 2011) proposed the initial construction of a SH scheme with unlink ability using a reusable certificate. In this model, the property credentials are issued by a certificate authority, which constructed a SH, in the standard manner, by adapting the identity-based encryption.

In most of the SH schemes, Group Authority (GA) who is not confirming to be the players belong to his own group or not, without revealing the member's ID. Consider a community supported by a social network service. In this a member of this community might want to know if his friend belongs to the same community and wants to communicate with the member secretly by initiating a SH. In this scenario, the GA need not know the member's ID. However, GA may want to know the number of executing handshake protocols and time when handshake protocols were initiated for each community to improve some service in this social service network. In this situation, the number of executing handshake protocols should be known to GA and a member's ID should not be known to GA.

The traditional and recent methodologies discussed in the above will suit well in wireless network, whereas it will not in WSN. As the WSN has limited resources, the executing GA, also termed as Target Authority (TA) should be lesser in size. Hence, this study proposed two authorities, called Secret Handshake Issue Authority (SHIA) and Secret Handshake Validate Authority (SHVA). These agents will occupy lesser memory space a defined the handshaking protocol, in order to solve energy drain attacks (Liu *et al*., 2011; Nam and Cho, 2012). The energy drain attack is injected to drain the energy of the sensor nodes, which is also called sleep deprivation attacks. The proposed work is described in the next section followed by brief introduction about energy drain attack.

The energy drain attacks are a form of denial of service attack whereby an attacker renders a pervasive computing device inoperable by draining the battery more quickly than it would be drained under normal usage. This may be injected in any of the following three main methods: (1) Service request power attacks- This is a form of attack where repeated requests are made to the victim sensor node for services and handshake, (2) Benign power attacks- This is an attack where the victim sensor node is forced to execute a valid but energy-hungry task repeatedly and (3) Malignant power attacks- This is another form of attack where the attacker modifies or creates an executable task in the sensor node to make the system for consuming more energy than normal energy consumption.

## 2.1. Proposed Work

The methodology and the security requirements of proposed Secret Handshake Issue and Validate Authority (SHIVA) are discussed in this section. In a secret handshake system, the following four types of entities in the group G are defined. To improve the security of the system, the role of existing Group Authority (GA) is divided into two elements, (1) Secret Handshake Issue Authority (SHIA) and Secret Handshake Validate Authority (SHVA). The various terms related to this proposed work are:

- A member is an entity who belongs to the group. U ∈ G means that U belongs to the group G
- Non-member: A non-member is an entity who does not belong to the group. U/∈ G means that U does not belong to the group G
- SHIA is responsible for adding users into his group. If a user is added to the group of SHIA, SHIA issues a certificate to the user
- SHVA is responsible for revealing users as well as checking whether handshake players belong to his own group. SHVA maintains a list of member IDs

Since a user sends his ID to SHVA in the member addition algorithm, SHVA has the list of member IDs with a handshake player tracing algorithm. SHVA can confirm whether a handshake player belongs to his group by revealing the ID used with a handshake player tracing algorithm. In existing Secret Handshake (SH) schemes with a handshake player tracing algorithm, it seems that GA needs to reveal member IDs to confirm whether a handshake player belongs to his group. Obviously, it is excessive that an ID is revealed to confirm membership. However, revealing of handshake players is useful if disputes arise.

SHIA and SHVA create the group G. SHIA issues a certificate to non-members and adds them to the group G. When a handshake protocol is executed, SHVA can check whether a handshake player belongs to G without revealing the player’s ID. However, SHVA cannot reveal a member’s ID alone. If a handshake player wants to know the handshake partner, A brings forth his own ID to SHVA and SHVA reveals the handshake partner by receiving A’s ID and secret information from A.

The implementation of this attractive scenario is explained hereunder, the pictorial representation of the proposed work is shown in **Fig. 1-3**. The **Fig. 1** is shown the functionality of adding a new member to the group. The **Fig. 2 and 3** show the validation of a secret handshake through validation agent.

A SHIVA consists of the following six algorithms:

- Setup: The common parameter generation algorithm. Given a security parameter k, Setup outputs the public parameters (param) that are common to all groups
- Key Gen: The group public/secret key generation algorithm. Key Gen is run by SHIA and SHVA. Given param, Key Gen outputs a group public key gpk, a secret key of SHIA isk and a secret key of SHVA tsk
- Add: Is the member addition algorithm. Add is executed by a non-member A and a SHIA. Given param, gpk and isk, Add outputs a membership certificate ($\text{cert}_A$), a secret key ($\text{sk}_A$) and ID of a (IDA)
- Handshake: Is the authentication protocol executed between two players A and B, based on the public input param. The group public keys (gpkA and gpkB), certificates (certA, certB) and secret keys (skA, skB) of A and B are input to Handshake. The output of the algorithm is either reject or accept. A
- Handshake ←→ B means the situation in which A and B execute Handshake. SHVA, B means a transcript that the handshake players A and B execute Handshake. A transcript SHVA, B of the handshake protocol is assumed to be known by SHIA and SHVA
- Group Trace: A handshake player’s group trace algorithm. Given gpk, tsk and a transcript TA, B, Group Trace outputs yes if A, B ∈ G; otherwise, Group Trace outputs no. This algorithm is executed by SHVA
- Request Reveal: The handshake player tracing algorithm. Given gpk, tsk, cert A, skA, a transcript TA, B and internal information that is used in Handshake by a player A, Request Reveal outputs the member B

## 2.2. Security Definitions

The introduction of Group Trace is to guard as much as possible against impostor non-members. In more detail, SHIVA should be satisfied that if a member A∈ G executes a Handshake with B ∈ G and outputs acc, Group Trace should output yes.

The introduction of Request Reveal is to strengthen a handshake player’s anonymity against a handshake partner and a trace authority as strongly as possible. In more detail: (b1) even an honest member A cannot reveal a handshake partner’s ID alone when A executes a Handshake; and (b2) even SHVA cannot reveal a handshake player’s ID alone. That is, a handshake player’s ID cannot be revealed without executing Request Reveal with both TA and a handshake player. For impersonator resistance, detector resistance and unlink ability, the same definition as in the ordinary SH schemes.

The salient feature of the proposed technique is that it establishes threshold number of session keys simultaneously between the user and individual sensor nodes during a single authentication process without using the public key cryptography. The proposed scheme therefore, reduces the computational complexity on one hand and enhances the security aspects on the other.

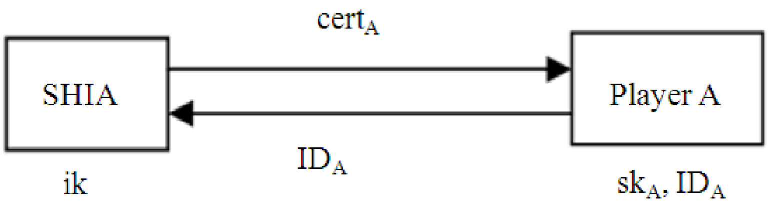

**Fig. 1.** Adding member through SHIA

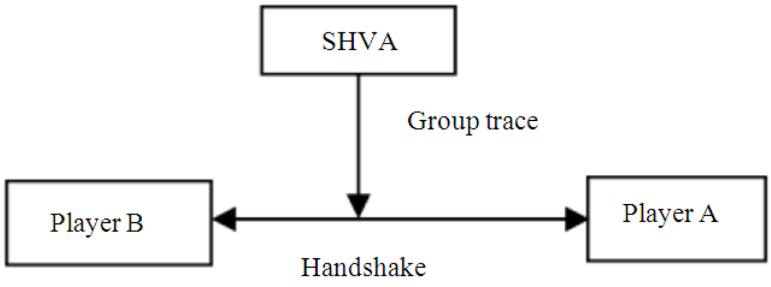

**Fig. 2.** monitoring handshake through Group Trace process of SHVA

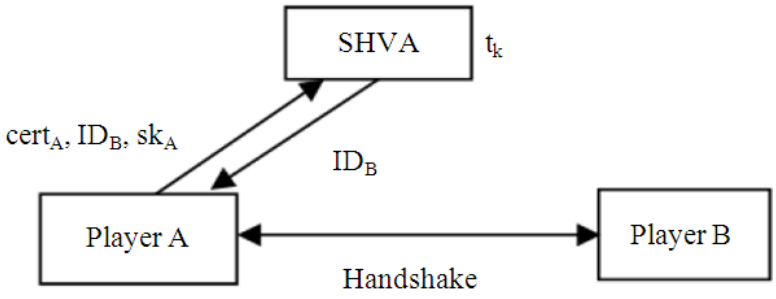

**Fig. 3.** Secret Authentication through SHVA

## 3. RESULTS AND DISCUSSION

The proposed SHIVA is compared with traditional Target Authority (TA) Model and Recent Mobile Agent (MA) model. The Reliability and scalability are major research issues in the design of networking protocol. Hence, the proposed works are analysed with respect to reliability and scalability and the result is compared with TA and MA. The reliability is computed based on the simulation data and result. The numbers of nodes are varied and numbers of attacker nodes are also varied for performance comparison. The simulation data is shown in the **Table 1**. The reliability when 10% of attacker node, 20% of attacker node and 30% of attacker node are shown in **Fig. 4-6**.

The scalability is observed from the above data, in which the system has 70% and above packet delivery ratio only accepted as scalable system. Hence, when 10% attacker nodes are inserted the TA supports up to 500 Nodes, whereas MA and proposed SHIVA support 1000Nodes. When attacker nodes increases, the TA supports up to 200 Nodes only, whereas MA supports 500 Nodes and proposed SHIVA support even for 1000Nodes.Similarly, the TA and MA supports only 100 Nodes when 30% of attacker nodes are inserted. The proposed system always supports above 80% packet delivery ratio. Hence, the proposed system proves better scalability than the existing systems.

In the present study three sets of attacks are created. Set 1 represents attacks based on traditional Target Authority (TA) model.

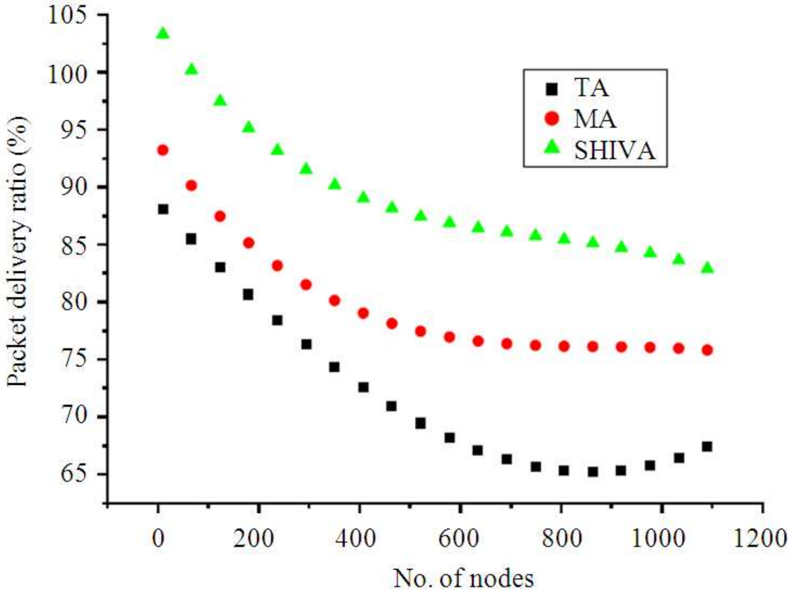

**Fig. 4.** Reliability at 10% attacker node

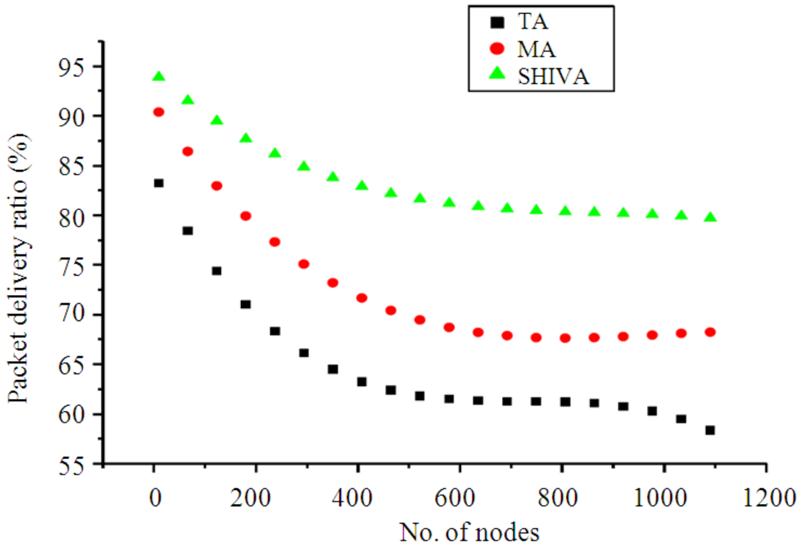

**Fig. 5.** Reliability at 20% attacker node

**Table 1.** Simulation environment

| Parameters | Values |
|---|---|
| Simulation time | 10 unit time |
| No of nodes | 100, 200, 300, 500 and 1000 |
| Attacker nodes | 10, 20 and 30% on total number of nodes |
| Reliability | In term of Packet Delivery Ratio (PDR) |
| Scalability | Model supports > 70% PDR |

Set 2 represents the attacks based on Mobile Agent (MA) model. Set 3 represents attacks based on SHIVA model. In all these models percent of packet delivery ratio is used to measure the percentage of uncompromised entities whose threat scores are below the threshold β at each step of an attack. The mean values across attacks are indicative of the information provided for the estimation of the attacks which have minimum threshold value at each step.

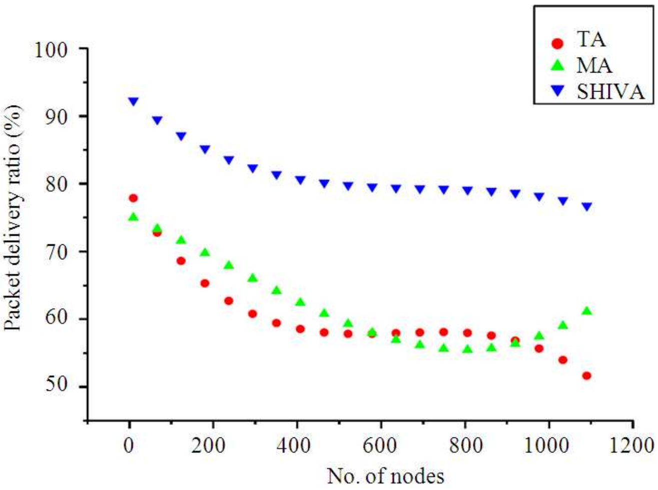

**Fig. 6.** Reliability at 30% attacker node

In the present study the threshold value is least in SHIVA compared to the other two attacks. Hence this method is far better than other two existing methods of attacks. The threshold value decreases from 25, 15 and 10 respectively and this is seen from the **Fig. 1-3** and thus the reliability at 30 % attacker node is achieved with the proposed scheme.

## 4. CONCLUSION

Secret Handshake issue authority SHIA and Secret Handshake Validate Authority are adopted in the present work occupy lesser memory space which is defined the handshake protocol and the aim of this is to reduce energy for the attacks. SHIVA model is compared with traditional Target authority model and recent Mobile agent model. SHIVA model stems out the best networking protocol and this is established from the reliability and scalability as evaluation parameters. The reliability using 10% of attacker nodes to 30% attacker node reveals that the threshold value decreases from 25 to 15 and then to 10 as the number of attacker nodes increases. The scalability ensures the accommodation of 1000 nodes in the case of SHIVA compared to MA model accommodating 500 nodes alone and this is much higher compared to TA model which can accommodate only 200 nodes. Thus the proposed system supports above 80% packet delivery ratio compared to the other two models.

## 5. REFERENCES

Dong, D.. M. Li, Y. Liu, X. Li and X. Liao, Topological detection on wormholes in wireless ad hoc and sensor networks. IEEE/ACM Trans. Network., 19: 1787-1796. DOI: 10.1109/TNET.2011.2163730

El-Khatib, K., 2010. Impact of feature reduction on the efficiency of wireless intrusion detection systems. IEEE Trans. Parallel Distributed Syst., 21: 1143-1149. DOI: 10.1109/TPDS.2009.142

Liu, Y., D. Dong, X. Liao, C. Shen and X. Wang, 2011. Edge self-monitoring for wireless sensor networks. IEEE Trans. Parallel Distributed Syst., 22: 514-527. DOI: 10.1109/TPDS.2010.72

Modares, H., R. Salleh and A. Moravejosharieh, 2011. Overview of Security Issues in Wireless Sensor Networks. Proceedings of the 3rd International Conference on Computational Intelligence, Modelling and Simulation, Sep. 20-22, IEEE Xplore Press, Langkawi, pp: 308-311. DOI: 10.1109/CIMSim.2011.62

Nam, S.M. and T.H. Cho, 2012. Energy efficient method for detection and prevention of false reports in wireless sensor networks. Proceedings of the 8th International Conference on Information Science and Digital Content Technology, Jun. 26-28, IEEE Xplore Press, Jeju Island, Korea, pp: 766-769.

Xiaowang, G. and Z. Jianyong, 2011. Analysis and design of energy-oriented security protocols for wireless sensor networks. Proceedings of the International Conference on Electronic and Mechanical Engineering and Information Technology, Aug. 12-14, IEEE Xplore Press, Harbin, Heilongjiang, China, pp: 2298-2301. DOI: 10.1109/EMEIT.2011.6023570