A DESIGN AND SIMULATION OF DISTRIBUTED TRUST MODEL FORWIRELESS SENSOR NETWORKS

S. Kiran Kumar
M.Tech (Pursuing)

R. Raja Kishore M. Tech
Associate Professor

Dr.M. Narsing Yadav Ph.D
Professor & HOD

Department of Electronics & Communication Engineering, Malla Reddy Institute of Engineering and Technology, Affiliated to JNTU- Hyderabad, Telangana

ABSTRACT

Now a days wireless sensor networks are rapidly growing technologies that have been widely used in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid, etc. However, the wireless media and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus providing security is extremely important for the safe application of WSNs.

Various security mechanisms like cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. To establish secure communications, we need to ensure that all communicating nodes are trusted first, according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated after that communication trust, energy trust and data trust are considered during the calculatio n of direct trust. Distributed trust model can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more effectively. A network Controller is designed to monitor network nodes continuously and if malicious node is found then it changes the routing path. By adding network controller to this model will reduces the packet drop ratio between nodes. Hence Performance of the model increases and Simulation results of Trust models are shown in output.

INTRODUCTION:

WSNS are emerging technologies that have been widely used in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid, etc. However, the wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs. Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes.

To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trustworthiness of another node. From the literature on this topic, we can find that: 1) In the current research work, the assessment of trust values for sensor nodes is mainly based on the communication (successful and unsuccessful communications) point of view. In fact, just considering the communication behavior, we cannot decide whether a sensor node can be trusted or not. Besides the communication behavior, other trust metrics such as the energy level should also be taken into account to calculate the trustworthiness of sensor nodes. In addition, an efficient trust model should deal with uncertainty caused by noisy communication c hannels and unstable sensor nodes' behaviors. 2) There are two common ways to establish trust in WSNs: calculating direct trust based on direct interactions and calculating indirect trust value based on recommendation from the third party. However, not all the third parties are trusty and not all the recommendations are reliable. Thus, a discriminate analysis about the third party and recommendation is essential. 3) Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. For example, in some routing protocols or localization algorithms sensor nodes need the information of the two-hop neighbor nodes to establish the routing or localize themselves. Therefore, providing the trust assessment for non- neighbor nodes becomes very important. 4) Because of the dynamic topology, the trust relationship between sensor nodes constantly changes in WSNs. Trust is a dynamic phenomenon and changes with time and environment conditions. However, most existing trust models do not solve the trust dynamic problem. The evolution of trust over time is another problem that needs further study. In order to solve the above- mentioned problems, we propose an efficient distributed trust model (EDTM). The proposed EDTM can evaluate the trust relationships between sensor nodes more precisely and can prevent security breaches more effectively.

2 ASSUMPTIONS AND NETWORK MODEL:

Scenario: In this paper, we consider a scenario in which all the sensor nodes are randomly deployed without mobility. As shown in Fig.1, there are three kinds of nodes in the network: subject nodes, recommender and object nodes. If a sensor node A wants to obtain the trust value of another sensor node B, the evaluating sensor node A is named as subject node and the evaluated node B is the object node. This paper is a multi- hop network which means that the sensor nodes can only directly communication with the neighbor nodes within their communication range. The packets exchanged between any two non-neighbor nodes are forwarded by other nodes. The forwarding node not only can just "pass" the packets from source nodes to destination nodes but also can process the information based on their own judgments. Generally, the trust value is calculated based on a subject's observation on the object and recommendations from a third party. The third party who provides recommendations is a recommender.
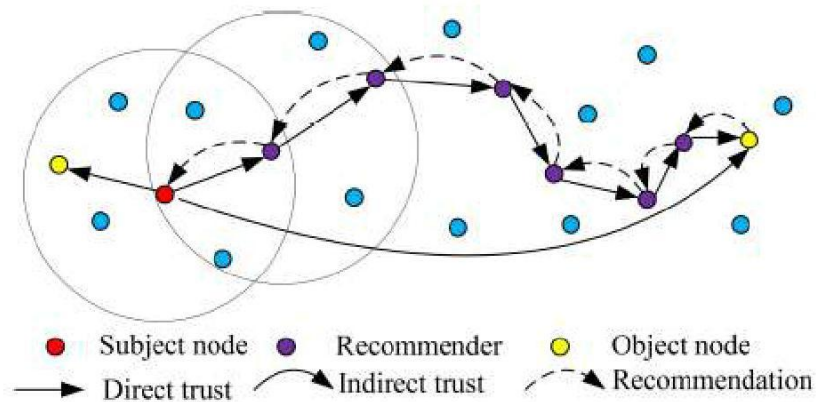
Node capability:

It assumes that sensor nodes have the same capability of computing, communicating and storing. Their communication ability is limited by specific wireless techniques. Only when two nodes move into each other's communication range could they detect each other and start communication. A homogeneous WSN is considered, that is all the sensor nodes have the same initial energy level and communication range. Additionally, in order to secure data transmission over the wireless network, each node is assigned a unique ID and a pair of public/private keys for encrypting and decrypting data, as well as with a public key certificate issued by some trustable Public Key Infrastructure (PKI). Each node keeps a list of neighbor nodes which stores their IDs and their communication information.

Attack model:

There exist many malicious attacks in WSNs, such as DoS attack, node replication, Sybil attack, wormhole attack, attacks on Information, etc. Moreover, it should be noticed that similar to most security schemes, a trust model is also vulnerable to many malicious attacks, such as bad/ good-mouthing attack and on-off attack. In a bad-mouthing attack, malicious nodes intentionally give dishonest recommendation to neighbor nodes. For example, they maliciously provide lower recommendation for normal ones during trust evaluation. Thus, recommendations under bad- mouthing attack cannot reflect the real opinions of the recommender. On the contrary, the sensor nodes conducting good mouthing attack intentionally provide higher trust value for malicious nodes. In an on-off attack, malicious nodes can behave good or bad alternatively. When the trust values of malicious nodes are significantly reduced, they can act well for a period to improve their trust values.
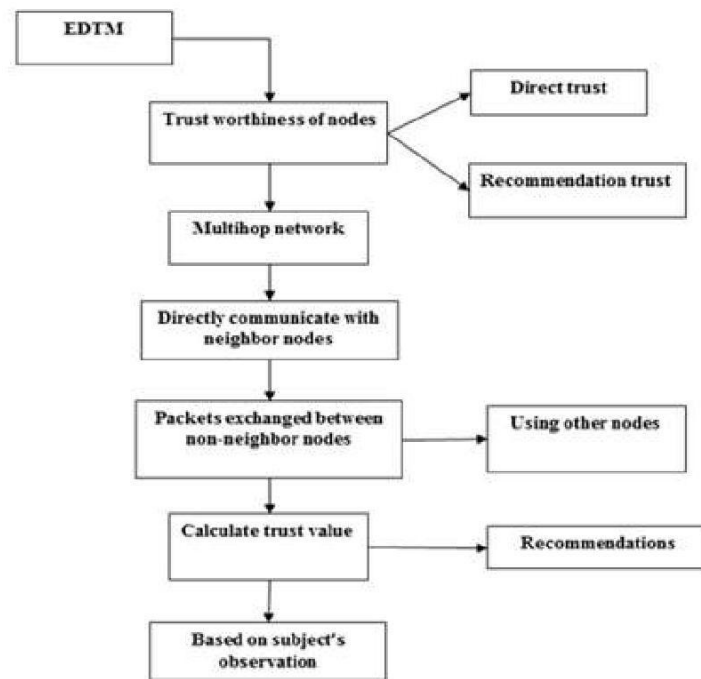
Figure: The EDTM structure

OVERVIEW OF EDTM:

To efficiently compute the trust values on sensor nodes, we first need a clear understanding of the trust definition and the various trust properties that are adopted in a trust model.

Definition and properties of Trust:

Trust: There are several definitions given to trust in the literature. Trust is always defined by reliability, utility, availability, risk, quality of services and other concepts. Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors.

That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs. In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 mea ns the opposite.

Direct Trust:

Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes.

Recommendation Trust:

As mentioned above, since the recommendations fro m third parties are not always reliable, we need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust.

Indirect Trust:

When a subject node cannot directly observe an object nodes' communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes. Based on previous work, we can conclude that there are three main properties of trust: asymmetry, transitivity and composability. Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A. Transitivity means the trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. The transitivity means the trust value can be passed along a path of trusted nodes. If node a trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. The transitivity is a very important property in trust calculation between two non-neighbor nodes. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value is a very important property in trust calculation between two non-neighbor nodes. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

The Structure of EDTM:

In this section, we describe the overall architecture of EDTM. When we say node B is trustworthy or untrustworthy for node A, there is a trust model between nodes A and node B. As shown in Fig.2, EDTM consists of two main components: one- hop trust model and multi- hop trust model which includes the following six components: direct trust module, recommendation trust module, indirect trust module, integrated trust module, trust propagation module and trust update module. When a subject node wants to obtain the trust value of an object, it first checks its recorded list of neighbor nodes. If the ID of the object node is in the list of neighbor nodes, the one-hop trust model is triggered. Otherwise, the multi- hop trust model is started. In the one-hop trust model, if the trust is calculated based on node B's direct experiences with node A completely, this model is called direct trust model. Otherwise, the recommendation trust module is built. In the multi- hop trust model, once the subject node A receives recommendations from other nodes about the object node B, indirect trust model can be established. In current trust models, the direct trust and recommendation are always used to evaluate the trustworthiness of sensor nodes. The direct trust is directly calculated based on the communication behaviors between two neighbor nodes. However, due to malicious attacks, using only direct trust to evaluate sensor nodes is not accurate. Thus, the recommendation from other sensor nodes is needed to improve the trust evaluation. In addition, if the number of communication packets between two neighbor nodes is too small, it is difficult to decide whether an object node is good or bad based on only few interactions. Therefore, in the one - hop trust model, we define a threshold of communication packets .If the communication packets between the subjects and object nodes are higher than the threshold, and then only the direct trust is calculated. Otherwise, the recommendations from the recommenders are needed for the object's trust evaluation. In the multi- hop trust model, the subject node first needs to select a set of recommenders. Then, the indirect trust is calculated based on recommendations and trust propagation. Next, we describe the detail calculation of direct, recommendation, and indirect trust.

TRUST CALCULATION IN EDTM:

Calculation of Direct Trust:

Unlike prior work, we compose our direct trust by considering communication trust, energy trust and data trust. The sensor nodes in WSNs usually collaborate and communicate with neighbor nodes to perform their tasks. Therefore, the communication behaviors are always checked to evaluate whether the sensor node is normal or not. The information on a sensor node's prior behavior is one of the most important aspects of the communication trust. However, communication channels between two sensor nodes are unstable and noisy, thus monitoring sensor node's behaviors in WSNs based on previous communication behaviors involves considerable uncertainty.

$$T_{com} = \frac{2b + u}{2} \qquad (1)$$

$$\text{where } b = \frac{s}{s+f+1}, \; u = \frac{1}{s+f+1}.$$

Calculation of the Ene rgy Trust:

Energy is an important metric in WSNs since sensor nodes are extremely dependent on the amount of energy they have. Malicious nodes always consume abnormal energy to launch malicious attacks. For example, malicious nodes which conduct DoS attack consume muc h more energy than normal nodes while selfish nodes consume less energy. Therefore, we use energy as a QoS trust metric to measure if a sensor node is selfish or maliciously exhaust additional energy

$$T_{ene} = \begin{cases} 1 - p_{ene}, & if E_{res} \geq \theta \\ 0, & else \end{cases} \qquad (2)$$

Calculation of the Data Trust: The trust of the data a ffects the trust of the network nodes that created and manipulated the data, and vice- versa, we introduce the evaluation of data trust in this section. The data packets have spatial correlation, that is, the packets sent among neighbor nodes are always similar in the same area. The data value of these packets in general follows some certain distribution, such as a normal distribution.

$$T_{data} = 2 \left(0.5 - \int_{\mu}^{v_d} f(x)dx \right) = 2 \int_{v_d}^{\infty} f(x)dx \qquad (3)$$

Calculation of the Recommendation Trust:

The recommendation trust is a special type of direct trust. When there are no direct communication behaviors between subject and object nodes, the recommendations from recommender are always taken into account for trust calculation. However, in most existing related works, the true and false recommendations are not distinguished. How to detect and get rid of false recommendations is important since it has great impact on the trust calculation.
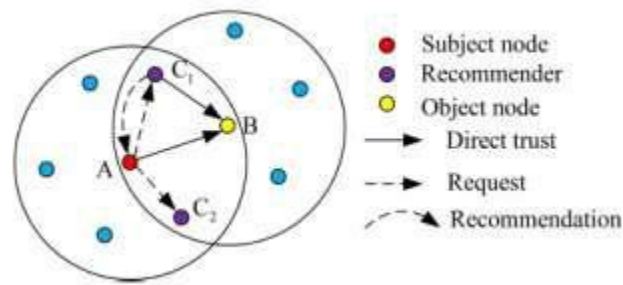
Figure: Calculation of recommended trust

Calculation of the Indirect Trust:

WSNs are multi- hop networks, when there are no direct communications between subject and object nodes, indirect trust can be established since trust is transitive. In this paper, the calculation of indirect trust includes two steps: 1) the first step is to find multi- hop recommenders between subject and object nodes, and 2) the second step is the trust propagation which aims at computing the direct trust. The path from the subject node to the object node established by the recommenders is named as Trust Chain.
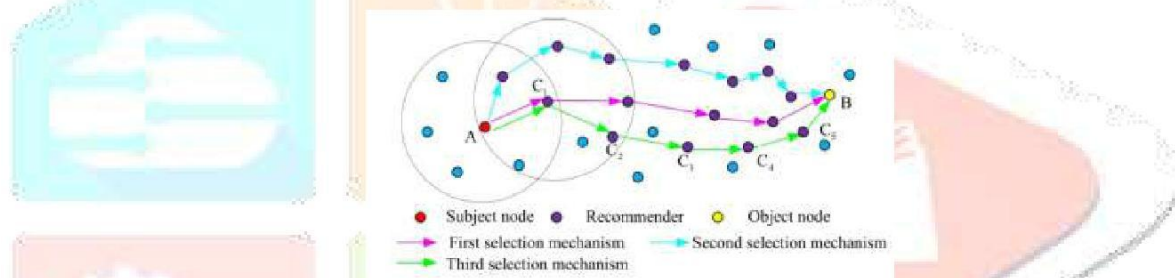
Figure: Calculation of Indirect Trust

Update of Trust value:

Due to the dynamic behavior of WSNs such as leaving or joining the network, the trust values of sensor nodes should be updated periodically. First, the trust value should not be updated too often. Because frequently updating the trust value will waste a lot of energy, and the trust evaluation will be easily affected by the network traffic conditions (e.g., congestion and delay). In addition, the update cycle time cannot be too long. A node's historical trust values should be taken into account to measure its current trustworthiness. If the cycle time is too long, it cannot efficiently reflect the current behaviors of the object node. To solve these issues, we use a sliding time window concept to update the trust value.

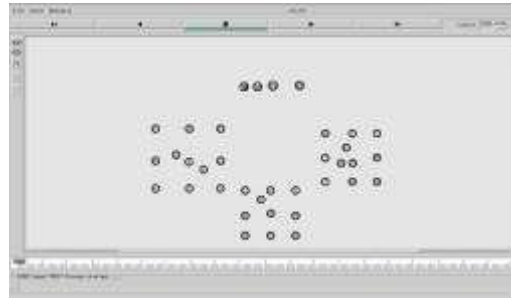## SIMULATION RESULTS AND ANALYSIS:
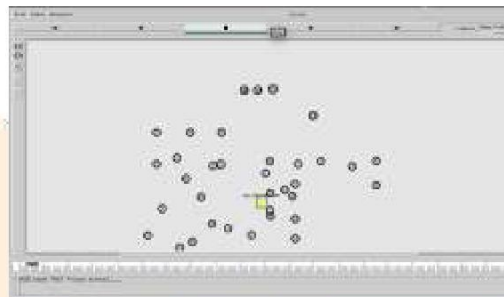

Figure: NAM window with 35 Nodes

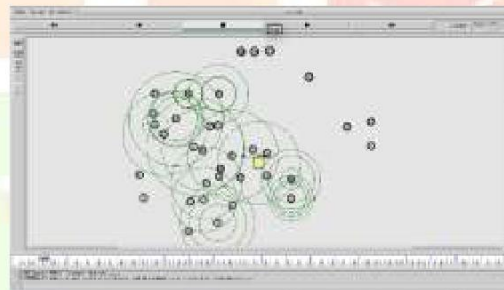Figure: One Node selected as a Network Controller
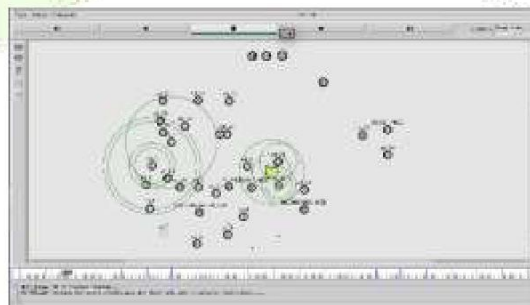

Figure: Execution of NAM started

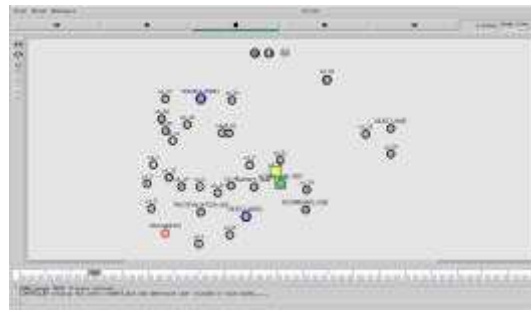Figure: Unique Ids assigned by the controller

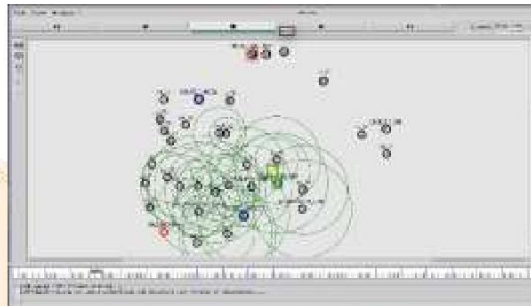Figure: Subject node and Object Node detected

Figure: Malicious Node detected in the network

Figure: Malicious Node using fake User ids to send malicious data into network

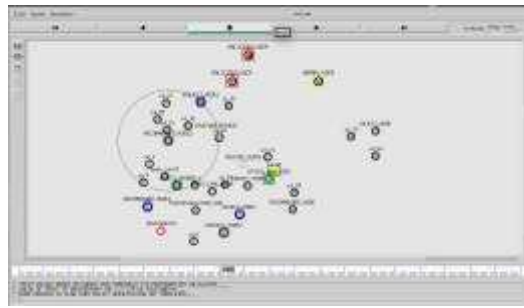Figure: Network Controller detected malicious node and blocked it.

Figure: Trust value has been calculated.
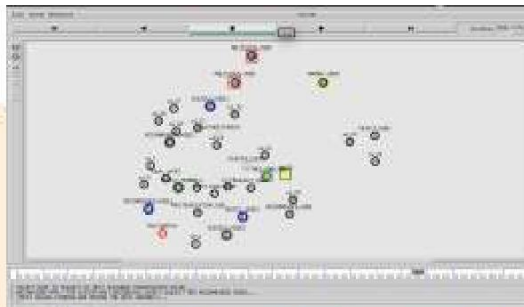

Figure: Trustworthy Nodes are detected.

Figure: Execution Finished
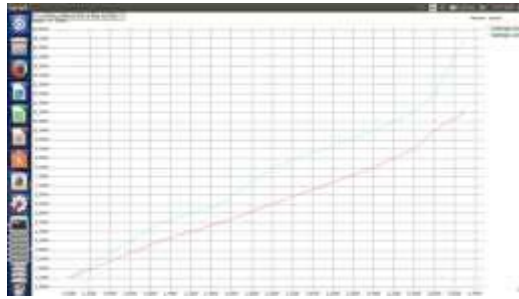

Figure: Performance dropping

Figure: Network Output

CONCLUSION:

The trust model has become vital for malicious nodes detection in WSNs. It can assist in several applications such as secure routing, secure data aggregation, and trustworthy key exchange because of the wireless options of WSNs, it needs a distributed trust model without any central node, where neighbor nodes will monitor one another in addition, an efficient trust model is required to handle trust connected data in a secure and reliable manner during this paper style and distributed and trust model is pla nned throughout this trust model, the calculation of express trust, recommendation trust and indirect trust area unit mentioned moreover, the trust propagation and update area unit studied.

Simulation results show in style associated distributed trust model and it's an economical and attack-resistant trust model. However, a way to choose the right price of the burden and therefore the outlined threshold continues to be challenge downside that we tend to arrange to address in our future analysis endeavors.

Future Enhancement:

Trust is an important factor in network models. Mostly trust is calculated between two nodes in the wireless sensor networks with centralized module. As wireless technology is rapidly growing nodes it can determine malicious data/malicious node for communication with other nodes and also by using feedback methodology we can improve the system performance. As we are monitoring continuously we can get feedback from the system and for the next iteration we can take precautions to reduce the packet drop so that performance will be **increased.**

REFERENCES:

[1] H. Chan and A.Perrig, "Security and Privacy in Sensor Networks".IEEE Computer, Vol. 36, No. 10, pp. 103-105, 2003.

[2] Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park, "Pervasive, Secure Access to a Hierarchicalbased Healthcare Monitoring Architecture in Wireless Heterogeneous Sensor Networks". IEEE Journal on Selected Areas of Communications, Vol. 24, No. 7, pp. 400- 411, May 2009.

[3] V.C. Gungor, L. Bin, and G.P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid". IEEE Transactions on Industrial Electronics, Vol. 57, No. 10, pp. 3557-3564, 2010

[4] G. Han, J. Jiang, L. Shu, J. Niu and H.C. Chao, "Managements and applications of trust in Wireless Sensor Networks: A Survey". Journal of Computer and System Sciences, pp. 1-16, 2013. [5] S. Ganeriwal, L.K.

Balzano and M.B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks". In Proceedingsof the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 66-77, 2004.

[6] Z. Yao, D. Kim and Y. Doh, "PLUS: Parameterized and Localized trust management Scheme for sensor networks security". IEEE Internationa l Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 437-446, 2008.

[7] R. Feng, X. Xu, X. Zhou and J. Wan, "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory". Sensors, pp. 1345-1360, 2011.

[8] G. Han, Y. Dong, H. Guo, L. Shu, D. Wu, "Cross- layer Optimized Routing in WSN with Duty-cycle and Energy Harvesting". Wireless Communications and Mobile Computing, 2013 accepted.

[9] G. Han, X. Xu, J. Jiang, L. Shu and N. Chilamkurti, "The Insightsof Localization through Mobile Anchor Nodes in Wireless Sensor Networks with Irregular Radio". KSII Transactions on Internet and Information Systems, pp. 2992-3007, 2012.

[10] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey". IEEE communications survey and tutorials, Vol.14, No. 2, pp. 279-298, 2012.