I J C T A, 9(2), 2016, pp. 943-950

Trust based Energy Efficient Scheme for Hierarchical Clustering in Wireless Sensor Networks

L. Ramalingam* **and S. Audithan****

Abstract: Trust model have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). However, most current research works consider only communication behavior to calculate sensor nodes trust value that is not enough for trust evaluation. Hence, we propose Trust based Energy Efficient Scheme for Hierarchical Clustering in Wireless Sensor Networks (TEEHC). In TEEHC, the calculation depends on Communication Trust and Energy Trust. The Energy Trust evaluates residual energy of each sensor and geographical average energy of all sensors in each cluster. The proposed TEEHC can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaks more effectively. The simulation results of TEEHC outperforms better throughput, reduce the energy consumption and improve the lifetime of the network.

Keywords: Trust, Energy, Clustering, Wireless Sensor Network.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) contains a large number of spatially disseminated small devices that cooperatively examine and respond to environmental conditions and send the gathered data to the Base Station (BS) using wireless channels. Different security mechanisms, for example cryptography, authentication, confidentiality and message integrity, are used to avoid security threats such as eavesdropping, message replay and falsehood of messages. These approaches still suffer from many security vulnerabilities, such as denial-of-service attacks and node capture attacks. The traditional security mechanisms can oppose external attacks, but cannot resolve internal attacks efficiently that are caused by the captured nodes. To establish secure communications, all the communicating nodes are guaranteed to be trusted. This highlights the detail that it is critical to establish a trust model allowing a sensor node to conclude the trustworthiness of another node.

In this paper, the Communication Trust and Energy Trust are always used to evaluate the trustworthiness of sensor nodes. The Communication Trust is calculated based on the interaction behavior of the sensor nodes. Thus, the Energy trust is required to improve the trust evaluation. Energy Trust is measured based on the residual energy and Geographical Average Energy of each sensor node. Therefore, the source transmits the data to BS through the trusted Cluster Heads (CHs).

The rest of this paper is organized as follows: In section 2, the overview of related work is studied. Section 3 describes the TEEHC technique. In section 4, the performance of the TEEHC is evaluated. Finally, section 5 concludes the paper.

2. RELATED WORKS

Trust computation and Management Systems (TOMS) [1] computes the unique trust computation model and the trust effectively for each node. This trust model can improve the security and reliability of the

* Research Scholar, Department of Computer Science and Engineering, St. Peter's University, Chennai, India

** Professor, Department of Computer Science and Engineering, PRIST University, Kumbakonam, India

network. It reduces the complexity of the traditional trust and improves the efficiency. Hybrid Energy Efficient Distributed clustering (HEED) [2] selects CHs according to node residual energy and node degree. This protocol aims to prolong the network lifetime and minimize the control overhead. It is very difficult to obtain the network lifetime bounds to ensure predictability. High Energy First clustering (HEF) [3] is used to obtain the optimal CH and maximize the network lifetime. In this algorithm, the node with maximum energy is selected as the CH. Therefore, the energy drainage rate is decreased and the packet delivery rate is increased.

The Node based Trust Management (NTM) scheme [4] is based on a Clustered mobile sensor network that introduces a trust of a node within local management strategy. In this scheme, a node's trust-based information is stored as a history on the node itself and managed by the local mobile agent of the node. This algorithm aims to elect trustworthy stable CHs that can provide secure communication via cooperative nodes. Towards Energy-Efficient Trust System [5] technique was used to maximize security in terms of trust accuracy and trust robustness. In this scheme, watchdog technique minimizes the overall risk and reduces its redundancy. The main concern of trust-aware decision-making mechanism [6] is to filter out the reported information from untrustworthy nodes. If the trustworthiness score of a node is below the threshold, the node is not considered as a potential interaction. In Ranking-Based Method [7], the trustworthiness value of a node is a real value between 0-1and the trustworthiness values can be used to rank the nodes in the communication network.

Agent-based Trust Management Model [8] introduced a distributed agent based trust management scheme. The agent node use watchdog mechanism to observe the behavior of sensor nodes and computes the trust routing. This trust management model detects the malicious sensor node and identifies the HELLO flood attack and packet dropping attack. Hybrid trust management model [9] was the combination of certificate-based and behavior-based approaches.

Trust management scheme for Resilient Geographic Routing (T-RGR) [10] monitors the behavior of one-hop neighbors. Using predefined threshold values in this algorithm makes this scheme non-adaptive. Also it is vulnerable against collaborative attacks. Reputation-based trust mechanism [11] calculates the trust based on reputation and they use Bayesian formulation for representing reputation of a node. It assumes that the node has enough interactions with the neighbors so that the reputation can reach a stationary state. Though the rate of node mobility is higher, reputation information will not be steady. Therefore, this scheme is not able to handle uncertain situations.

Reputation-based framework for high integrity sensor networks [12] uses the watchdog mechanism to build trust rating. However, the watchdog cannot record all the behavior due to its own fault, so there is some uncertainty events in the trust system. A lightweight Group-based Trust Management Scheme (GTMS) [13] reduces the cost of trust evaluation. GTMS detect and prevent malicious, selfish and faulty nodes and it requires less memory, energy and communication overheads for WSN. Trust Management Architecture (TMA) [14] introduces a trust varying function that gives greater weight to the most recently obtained trust values in the trust calculation. This scheme minimizes communication and storage overheads. However, the main drawback of this approach was high false probability.

3. PROPOSED SYSTEM

In this paper, we propose Trust based Energy Efficient scheme for Hierarchical Clustering in WSNs (TEEHC). TEEHC aims to minimize the energy cost and maximize the security in WSN. This network consists of a BS, CHs and numerous sensor nodes that are grouped into clusters. Here all sensor nodes are stationary and locations and communication range of nodes are known. The clusters of sensors can be formed based on the location. Each cluster includes the CH and a set of sensor nodes. Each sensor has two main functions sensing and relaying. Sensors probe their environment and gather data. Then they transmit the collected

information to the CH directly in one hop or by relaying via a multi hop path. A CH is in charge of its cluster. It is assumed that each CH can reach and control all the sensors in the cluster. Every CH receives the information from different sensors, processes the data to extract relevant information and then sends it to the BS via multi-hop transmission**.** Therefore, the CH has higher computation power and memory when compared to other sensor nodes.

The information on a sensor node's prior behavior is one of the most important aspects of the communication trust [15]. 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. The communication trust is calculated based on successful and unsuccessful communication packets.

The Communication Trust of every node is calculated in equation 1

$$TC_i = \frac{2m + n}{2} \tag{1}$$

Where $m = \frac{s}{s + us + 1}$

$$n = \frac{1}{s + us + 1}$$

$s \rightarrow$ Successful communication packet

$us \rightarrow$ Unsuccessful communication Packet

In this paper the Energy Trust is calculated based on the residual energy and Geographical Average Energy of each sensor node. Geographical Average Energy of node is calculated by following formula.

$$GAE(r) = \frac{\sum_{i=1}^{cn} RE_i(r)}{cn} \tag{2}$$

$r \rightarrow$ Cluster round Number

$RE_i(r) \rightarrow$ Residual Energy

$cn \rightarrow$ Number of nodes in the Cluster

The Trust Energy is obtained from the equation (3) below.

$$TE_i = p\frac{E_i(r)}{GAE(r)} \tag{3}$$

$p \rightarrow$ Desired percentage of CH

The overall Trust of each node is evaluated by equation (4) below.

$$T_i = \frac{TC_i + TE_i}{2} \tag{4}$$

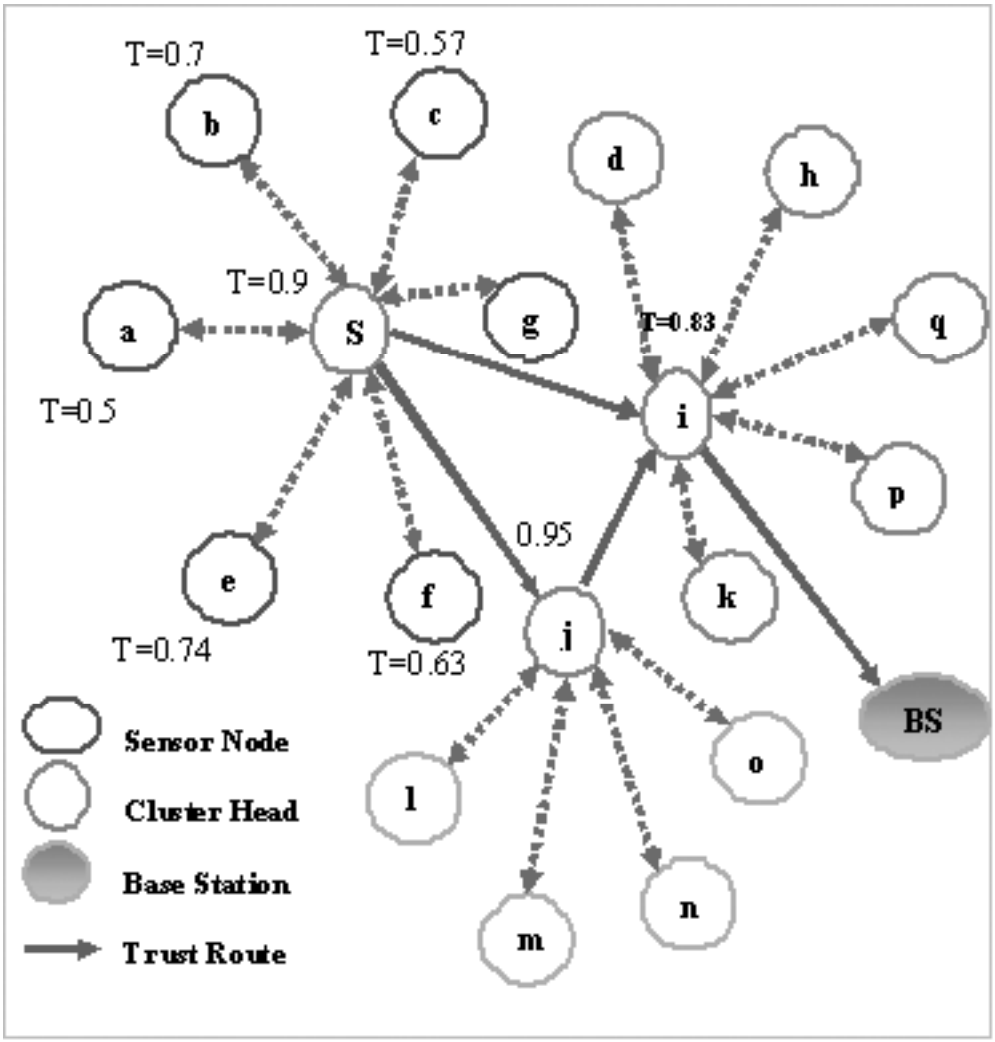

Figure 1: Illustration of Trusted Route

TEEHC selects the CH based on the threshold that is calculated by the suggested percentage of CH for whole network. In each round, the trust probability values ranges between 0-1. The Threshold value is determined in equation (5).

$$THi = \frac{T_i}{1 - T_i(r \bmod 1/T_i)} \qquad if\ i \in S \tag{5}$$

Where

$S \rightarrow$ Sensor nodes that not does not select the CH in previous round

The figure 1 shows that the illustration of the trust routing in WSN. The CH is chosen based on Communication trust and Energy Trust of each sensor node. If the Trust value is greater than the Threshold, that node is selected as a CH. The Source transmits the data to BS through the trusted CH node. The trusted path does not choose the untruthful nodes therefore the source transmit secure data to BS.

The figure 2 describes the flowchart of TEEHC scheme. In this scheme, the clusters are formed based on the location. Every sensor node computes the Communication Trust and Energy Trust. The Communication Trust value is calculated based on the successful and unsuccessful communication packets. The Energy Trust is estimated based on the Residual energy and Geographical Average Energy. If the Trust value is greater than the threshold, that node is selected as a CH. Finally, the sensor node transmits the data to BS through the trusted CH.

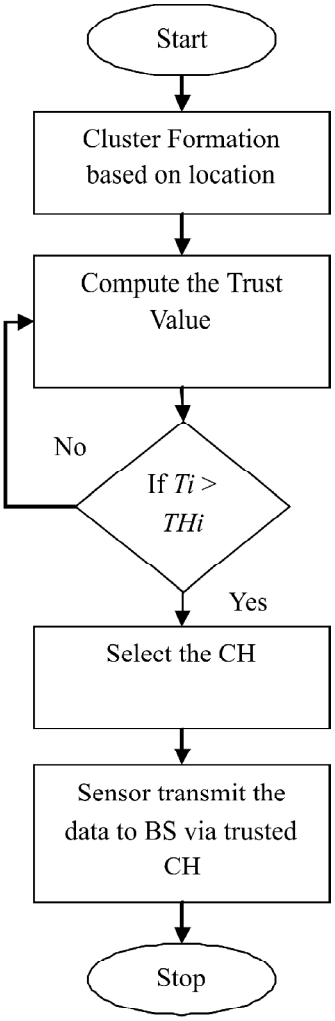

Figure 2: Flowchart of TEEHC

4. SIMULATION ANALYSIS

Network simulator is used to perform simulation between the TMA and the TEEHC protocols. NS-2 used programming in Object Oriented Tool Command Language (OTCL) and C++ for simulation of various wired and wireless scenarios. Both the protocols discussed here are simulated with the parameters indicated in the Table1.

Table1
Simulation Parameters of TEEHC Scheme

Parameter	*Value*
Simulation Area	1200 × 800m
Number of Nodes	50
Simulation Time	100ms
Channel Type	Wireless Channel
Radio Propagation model	Two Ray Ground
Network interface type	Wireless Phy
MAC Type	IEEE 802.11
Interface Queue Type	Pri Queue
Link Layer Type	LL
Antenna Model	Omni Antenna

4.1. Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. The PDR is calculated by Equation 6.

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \tag{6}$$

The figure 3 shows the PDR of the proposed scheme TEEHC is higher than the PDR of the existing method TMA. The greater value of PDR means the better performance of the protocol.

4.2. Packet Loss Rate

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The formula used to calculate the PLR is given in Equation. 7.

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \tag{7}$$

The PLR of the proposed scheme TEEHC is lower than the existing scheme TMA in Figure 4. Lower the PLR indicates the higher performance of the network.

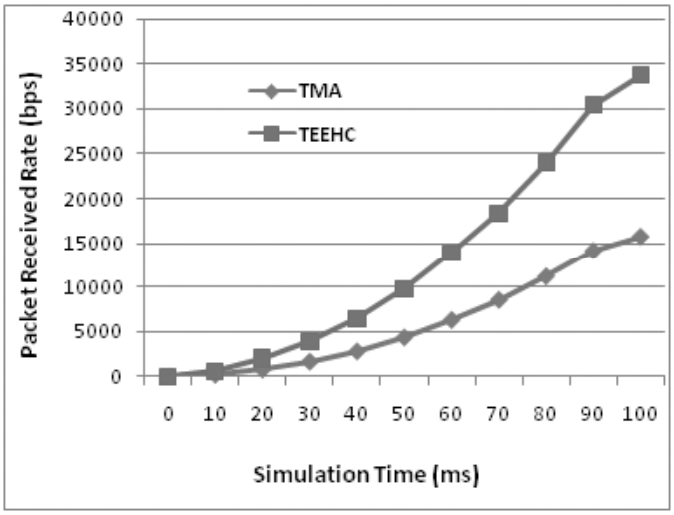

Figure 3: Packet Delivery Rate of TMA and TEEHC

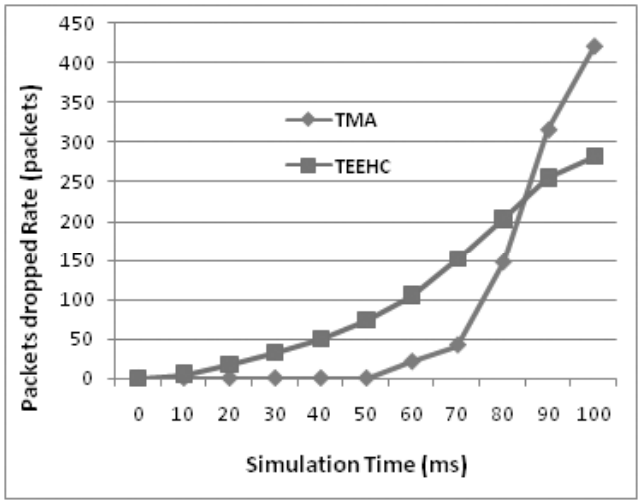

Figure 4: Packet Loss Rate of TMA and TEEHC

4.3. Average Delay

The average delay is defined as the time difference between the current packets received and the previous packet received. It is measured by Equation. 8.

$$Delay = \frac{\sum_{0}^{n} Pkt\ Send\ Time - Pkt\ \mathrm{Re}cvd\ Time}{Time} \tag{8}$$

Figure 5 shows that the delay value is low for the proposed scheme TEEHC than the existing scheme TMA. The minimum value of delay means that higher value of the throughput of the network.

4.4. Throughput

Throughput is the average of successful messages delivered to the destination. The average throughput is estimated using Equation. 9.

$$Throughput = \frac{\sum_0^n Pkts\ Received\ (n) * Pkt\ Size}{1000} \quad (9)$$

Figure 6 shows that proposed scheme TEEHC has greater average throughput when compared to the existing scheme TMA.

4.5. Residual Energy

The amount of energy remaining in a node at the current instance of time is called as residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations.

Figure 7 shows that the residual energy of the network is better for the proposed scheme TEEHC when compared with the existing scheme TMA.

5. CONCLUSION

In this paper we introduced a Trust based Energy Efficient Scheme for Hierarchical Clustering in Wireless Sensor Networks (TEEHC) to improve the CH process and maximizing the lifetime of the network. In this

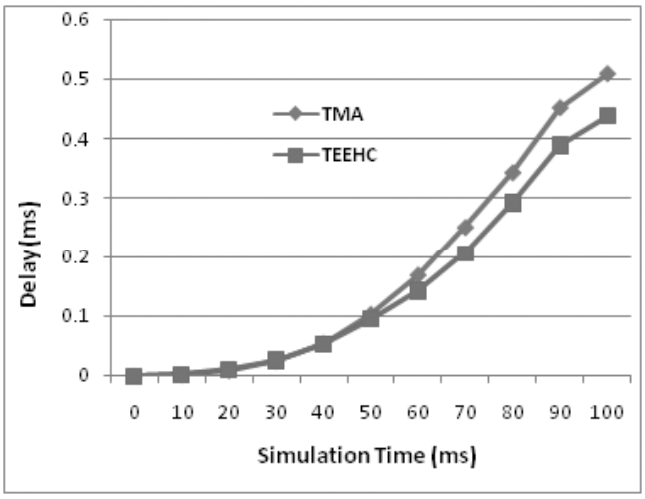

Figure 5: Delay of TMA and TEEHC

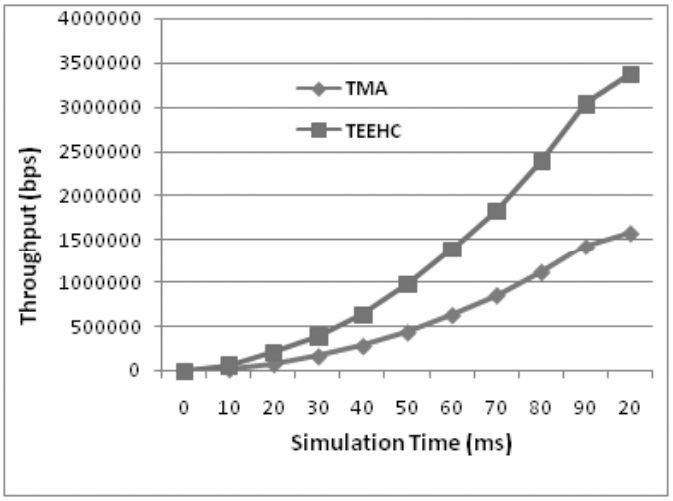

Figure 6: Throughput of TMA and TEEHC

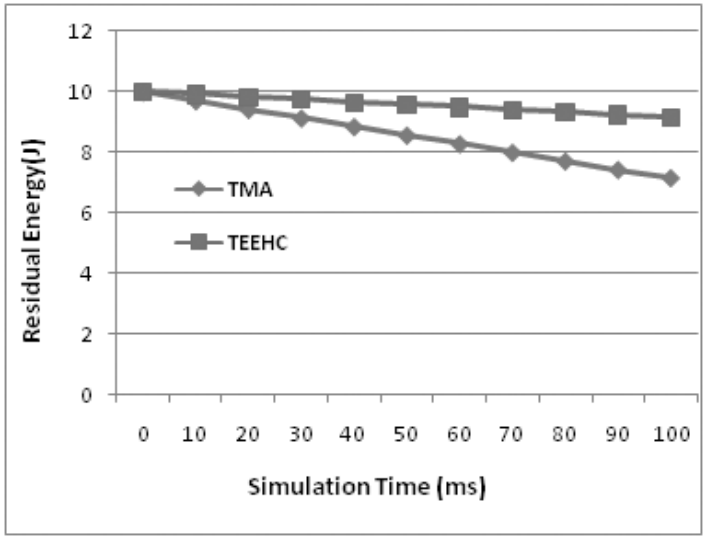

Figure 7: Residual Energy of TMA and TEEHC

scheme, the trust value is calculated based on the Communication Trust and Energy Trust. The Energy Trust evaluates the residual energy of each sensor and geographical average energy of all sensors in each cluster. The Energy Trust estimation is used to increase the energy efficiency of the network. It can be concluded from the simulation results that trust based routing increases the packet delivery rate and reduce the energy consumption in the communication network.

REFERENCE

[1] Yonglin Ren and Azzedine Boukerche, Modeling and Managing the Trust for Wireless and Mobile Ad hoc Networks, IEEE International Conference on Communications, (pp. 2129-2133), 2008.

[2] Ossama Younis and Sonia Fahmy, Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. vol. 1, 2004.

[3] Bo-Chao Cheng, Hsi-Hsun Yeh, and Ping-Hai Hsu, ¯Schedulability Analysis for Hard Network Lifetime Wireless Sensor Networks With High Energy First Clustering, in IEEE Transactions on Reliability, vol. 60, no. 3, September 2011.

[4] Raihana Ferdous, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan, Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks, IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 589-596, 2011.

[5] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou and J. C. M. Teo, Towards Energy-Efficient Trust System through Watchdog Optimization for WSNs, IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, March 2015.

[6] H. Dai, Z. Jia, and X. Dong, Ban entropy-based trust modeling and evaluation for wireless sensor networks,[in Proc. Int. Conf. Embedded Softw. Syst., 2008, pp. 27–34.

[7] F. Almenarez, A. Marin, D. Diaz, and J. Sanchez, B, Developing a model for trust management in pervasive devices, in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshops, Washington, DC, 2006, p. 267.

[8] H. Chen, H. Wu, J. Hu and C. Gao, "Agent-Based Trust Management Model for Wireless Sensor Networks," Multimedia and Ubiquitous Engineering, 2008. MUE 2008. International Conference on, Busan, 2008, pp. 150-154

[9] Efthimia Aivaloglou, Stefanos Gritzalis, Hybrid trust and reputation management for sensor networks, Wireless Network, Springer,16:1493–1510,2010.

[10] K. Liu, N. Abu-Ghazaleh, and K.-D. Kang, "Location Verification and Trust Management for Resilient Geographic Routing," J. Parallel and Distributed Computing, vol. 67, no. 2, pp. 215-228,2007.

[11] H. Chen, H. Wu, X. Zhou, and C. Gao, "Reputation-Based Trust in Wireless Sensor Networks,"Proc. Int'l Conf. Multimedia and Ubiquitous Eng. (MUE '07), pp. 603-607, Apr. 2007.

[12] Ganeriwal and M. Srivastava. "Reputation-based framework for high integrity sensor networks". In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), pp. 66-77, Oct 2004.

[13] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee Young-Jae Song, Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks, IEEE Transactions on Parallel And Distributed Systems, Vol. 20, No. 11, pp. 1698-1712, 2009.

[14] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan and Abdul Sattar A Trust Management Architecture for Hierarchical Wireless Sensor Networks, 35th Annual IEEE Conference on Local Computer Networks, 2010.

[15] Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. "An efficient distributed trust model for wireless sensor networks." Parallel and Distributed Systems, IEEE Transactions on 26.5 (2015): 1228-1237.