Secured Fuzzy Based Routing Framework for Dynamic Wireless Sensor Networks

I. Sakthidevi
Student
Anna University, Madurai Regional Centre
Madurai, Tamilnadu, India
sakthidevi.12@gmail.com

E. Srievidhyajanani
Assistant Professor
Anna University, Madurai Regional Centre
Madurai, Tamilnadu, India
esrievidhya@gmail.com

***Abstract*— Wireless sensor networks (WSN) are the ideal domain for applications involving critical security events like military surveillance and detection of forest fire. Wireless sensor networks involve multi-hop routing and it offer minor security against identity deception through replaying routing information. The trust factor in the routing environment plays an important role in the military surveillance and related applications. Secured data aggregation is an important criterion that attracts serious research work. The factors reasonable in such harsh WSN are increased complexity, high overhead and poor link quality in case of various cryptographic techniques. These problems need to be addressed and overcome with the help of appropriate framework mechanisms. The analysis is further enhanced by mobile and harsh network conditions. Current trust-aware routing protocols using traditional cryptographic techniques are not capable of effectively tackling this serious problem. To secure the WSN and to regularise the multi-hop routing techniques, the present work has been designed and implemented. A Fuzzy Based Trust-Aware Routing Framework (FBTARF) is the proposed method for security improvisation in dynamic WSN. FBTARF provides energy-efficient routing and reliable trust using fuzzification methods. Also, FBTARF provides the effective solution against harmful attacks due to identity deception. The dynamic nature of FBTARF is analysed by means of detailed evaluation using simulation and empirical experimental procedures. This has been studied for large-scale WSN under various environments including mobile and harsh network conditions. To improvise the security parameters, the proposed work is developed using a Fuzzy Based Trust Model which simultaneously considers multiple constraints and provides better security and energy conservation. The secured FBTARF model also provides effective and efficient routing in the dynamic wireless sensor network environment. Then, the comparison analysis based on normal TARF and Secured Fuzzy based trust aware routing framework (FBTARF) model is developed and the results show that the secured fuzzy model provides better results in terms of security, packet delivery ratio and energy conservation.**

***Keywords*— Energy, Fuzzy, Security, Trust Awareness, WSN**

I. INTRODUCTION

Wireless sensor networks (WSN) [2] are the domain mostly engaged in military surveillance and detection of forest fire. Battery-powered senor nodes are interconnected with tremendously limited processing capabilities in WSN. A sensor node or device connected in a WSN environment sends information to the destination through the multi-hop routing path within the coverage area of allotted radio communication range. This multi-hop routing often becomes victim for the suspicious malicious attacks. An attacker may intrude the nodes physically, collide with the sensor nodes during transmission, drop the data messages or misdirect messages in the intermediate route path or block the communication channel by jamming the radio interference [3].

Due to identity inception, the attacker can launch various unidentifiable attacks and malicious intrusions which are hard to detect during the normal course of transmission [4]. This research paper deals with various kinds of attacks where in the intruders mislead the network traffic and messages by identity deception through routing information change. In terms of security, WSN is one domain which is more vulnerable to various attacks. In order to achieve better security, several works have been proposed in the related area but the integration parameters for various attack detection and control are still in the initial stages [5][6].

WSN exhibits various characteristics such as tree-structured routing, computation and phased transmission periods, data aggregation mechanisms, in-network filtering methods and acceptable failures. Due to the mobility in wireless sensor networks, the harm of various malicious attacks based on the technique of replaying routing information is further exaggerated and the network behaviour becomes aggressive. Although mobility concept is for efficiesnt data collection, it greatly increases the chance of communication between the actual sensor nodes and the attackers as shown in various applications [8][9][10][11].

Minimising energy conservation and the medium access layer arguments are the main criteria to be considered for data aggregation using distributed processing. For effective Routing analysis, data aggregation is the vital parameter. In data aggregation, the following steps are to be followed. Merging all the information from various sources, routing and removing the duplicate information, minimising the transmission number and conserving the energy are the salient features of data aggregation. By means of data aggregation process, redundancy of data from other sensor nodes can be prohibited. Data Extraction is also possible from the raw data. Another important factor is sustaining high occurrence to preserve energy for a long lifetime in the network [6].

978-1-4673-4922-2/13/$31.00 ©2013 IEEE

A. *Secured Fuzzy with Trust Aware Data Aggregation*

Security related problems in data aggregation are follows as in [7]

1). Data privacy

Data privacy is achieved by transferring sensitive data which are subjected to passive attacks. With reference to security, data privacy is the most basic parameter, mainly in defensive environment such as wireless networks which are very vulnerable to eavesdropping. Various cryptography techniques can maintain privacy but the hurdle is complex encryption and decryption process involved such as modular multiplications includes several public key based cryptosystems but these algorithms consume power at high rate.

2). Data Reliability

The alteration occurred in the aggregated value of attacked source node or the aggregator node can be avoided by maintaining data integrity. The sensor nodes are compromised mainly because of the shortage of effective tampering resistant hardware. Even such hardware are present, it will be undependable. For better data reliability, secure data aggregation can be carried out in following two methods:

- . Hop-by-Hop encrypted data aggregation security
- End-to-End encrypted data aggregation security

Considering the existing methods for secure data aggregation, the following problems are observed:

- High transmission overhead
- High data complexity
- Complex encryption process
- High bandwidth occupancy
- Poor reliability
- Poor data confidentiality
- Poor data integrity

To overcome these problems, secured fuzzy based trust aware routing framework is implemented for the data aggregation process in WSN environment.

II. DESIGN OF FBTARF

For each node N in a WSN, to identify the certain known neighbours, a table called neighbourhood table with trust, energy cost and distance values are maintained. For analysis of these values, three parameters, viz. *Energy Watcher* and *Trust Manager* and *Distance Estimator* run on every sensor node. Observation and Recording of the energy cost for each known neighbour is done by *Energy Watcher*. This is based on the surveillance of the node N, during its one-hop transmission to reach the neighbours and the energy cost report from those neighbours. At times, a node which is compromised may wrongly report an extremely low energy cost to entice its neighbours into selecting that compromised node as their next-hop node. However, when fuzzification is implemented, FBTARF-enabled neighbours eventually abandon that compromised next hop node based on its low trustworthiness as tracked by *Trust Manager*. *TrustvManager* is responsible for tracking trust level values of neighbours based on network loop discovery and broadcast messages from the base station about data delivery. Once N is able to decide its next hop neighbour according to its neighbourhood table, it sends out its energy report message. The energy cost is broadcast to all its neighbours in order to deliver a packet from the node to the destination. For energy cost computation, following methods are used by *Energy Watcher*. Such an energy cost report also serves as the input of its receivers' *Energy Watcher*. *Distance Estimator* is responsible to calculate the distance from node to the cluster head.

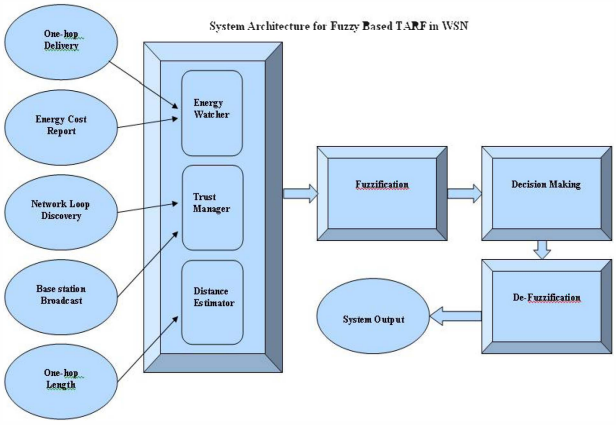

Fig. 1 System Architecture for Fuzzy Based TARF in WSN

III. RESOURCES AND METHODS

A. *Trust Based Clustering*

In the wireless network, cluster head is chosen by the sensor nodes based on the link connectivity among the nodes. The nodes which have higher link connectivity when compared with its two-hop neighbours are selected as cluster head. These cluster heads then transmit an advertisement message to all its neighbouring nodes. The normal nodes have to trace the information contained in the advertisement message. The advertisement message normally contains the cluster-head ID and location information of the cluster head. The normal nodes trace the information within their radio range.

Communication has to be established between the cluster head and normal nodes. For this, each normal node chooses one of the advertisement messages as its cluster head by means of strongest Received Signal Strength (RSS) and transmits a information called as member message back to the selected cluster head. The current energy status of the normal node and its ability of being a cooperative node is added into the message. Also, the information related to reliability value, unreliable sensing count, reliable sensing count and fuzzy trust value of the node are also added to the message. For the identification of the nearest neighbour cluster head, consider two cluster heads x and y. If an advertisement message signal is obtained at a cluster head x from another cluster head y, and y has a higher RSS value than the threshold value, then cluster head y will be considered as the neighbour cluster head and the ID of cluster head y is stored.

B. *Energy Cost*

In wireless communications, normally two models are used, free space channel model and radio model. If the communication distance d is lesser than the distance threshold d0, then free Space channel model is used. Else multi-path fading model is used as in [12]. For transferring k-bit message over a distance of d, the energy consumed is calculated by the radio model.

$$E_{trans} = E_{elec}(k,d) + E_{amp}(k,d)$$
$$= k * E_{elec} + k * \varepsilon_{fs} \quad (d < d0)$$
$$= k * E_{elec} + k * \varepsilon_{mp} \quad (d >= d0)$$

Where,

k = The number of forwarded bits for a distance d,

E_{elec} = The transmitter circuitry dissipation per bit, and

ε = The transmit amplifier dissipation per bit.

The receiving cost is computed by following equation

$$E_{recie} = k * E_{elec}$$

Dropping the network energy cost in WSN to increase the lifetime is shown in the following mathematical Model equation:

$$E_{total} = E_{trans} + E_{recie} + E_{process} + E_{sense}$$

Where:

E_{total} = Total network energy cost

E_{trans} = The transmission cost

E_{recie} = The receiving cost

$E_{process}$ = The energy cost while processing

E_{sense} = The energy cost while sensing

Finally the total energy cost is calculated by the minimum of energy cost of the transmitting distance. The minimum distance of the node to the cluster head is calculated and that is denoted by following equation

$$Min\ (E_{total})$$

C. *Trust Calculation*

Trust value is calculated by reliable and unreliable of the nodes For instance, the cluster possess 5 sensor nodes i.e., n1, n2, n3, n4 and n5. Then the distance between the successive nodes is calculated as d1, d2, d3, d4 and d5. The average of the values is calculated, $\eta 1$ and compared with threshold value, $\delta 1$ of the cluster. For instance, the cluster possesses 5 sensor nodes i.e., n1, n2, n3, n4 and n5 and the difference between the successive readings of every node is r1, r2, r3, r4 and r5. Then the average value $\eta 2$ of the readings is compared with its threshold value, $\delta 2$ of the cluster. If $\eta 1 > \delta 1$ and $\eta 2 > \delta 2$, then the nodes are unreliable. If $\eta 1 < \delta 1$ and $\eta 2 < \delta 2$, then the nodes are reliable. Two counters called reliable sensing watcher and unreliable sensing watcher are maintained, for the values of $\eta 1$ and $\eta 2$. It indicates the reliability of the sensor node. The sensor nodes can be classified as malicious or compromised node based on the reliability factor. Thus it helps in maintaining the network data away from that of the malicious nodes. This factor is estimated using the formula:

$$RV_i = RSW_i - URW_i / RSW_i + URW_i$$

Where:

RV_i = The reliable value of node i ($1 \leq i \leq k$)

RSW_i = The reliable sensing watch of node i

URW_i = The unreliable sensing watch of node i

D. *Packet Delivery Rate Calculation*

It denotes the information related to the communication ratio. The egotism and the regularity of the sensor nodes is indicated by this factor:

$$PDR_i = STR_i - PFR_i / STR_i + PFR_i$$

Where:

PDRi = The packet delivery rate of the sensing count node I is $1 \leq i \leq k$

STRi = The success count of the packet delivery rate of the node i

PFRi = The failiure count of the packet delivery rate of the node i

E. *Residual Energy Calculation:*

It indicates the residual energy of the sensor node in the network. The fall down of the biased battery can be eliminated by working out according to the selected residual energy factor. This in turn minimizes the further procedures required to process the power running strategies.

R_i is the Residual energy value of the node i where $1 \leq i \leq k$

The Total Trust Value (**TTV**) of the node i is calculated as follows:

$$TTV = W_1 R_i + W_2 PDR_i + W_3\ RV_i / W_1 + W_2 + W_3$$

F. *Power Consumption*

The battery value represents the power in the nodes. Each sensor node broadcasts quantification value of its own Pi:

$$Pi : -1 \leq P \leq 1$$

The cluster head now evaluates the rank of the node in order to select the nodes for data Aggregation. For this purpose, fuzzy logic is used.

1). Fuzzy logic

The troubles involving QoS can be established by the pro-active technique provided by the fuzzy logic. The working of a very dynamic nonlinear scheme such as a WSN, not in need of the system mathematical model can be handled professionally by fuzzy logic [14]. Applications similar to control systems, decision making, pattern recognition and system modeling make use of the fuzzy if-then rules. Three stages are involved in the fuzzy rule based inference algorithm.

- Fuzzy corresponding: the degree to the input fundamental steps and state of the fuzzy logic are determined
- conclusion: on the basis of the degree of competition, the conclusion of the rule is determined
- grouping: the result obtained by every fuzzy rules are combined together into a single overall result [13]

2). Rule Description

A fuzzy set A in X is characterized by a membership function which are effortlessly implemented by fuzzy conditional statements. In the case of fuzzy statement if the

precursor is true to some degree of membership then the resulting is also true to that same degree.

3). *The Rule Arrangement*

"If antecedent, then consequent**"**

The Rule: If distance and power consumption are low and trust is high then output is gentle else output is cruel. The fuzzy Logic in decision making uses the following technique. In this study, the fuzzy if-then rules consider the parameters: distance, power consumed and trust for evaluating the nodes. These are the three parameters which depicts the fuzzification analysis for the secured WSN in harsh and hostile environments. For the three inputs: distance, power consumed and trust, the resulting possibilities are Best Node (BN), Normal Node (NN) and Worst Node (WN). Here the inputs can take 2 values: Less and High. Hence the total number of outputs in this case is $2^3 = 8$. The basic criteria for selection is such that distance and power consumption values are to be lesser but trust value is to be higher. The first parameter, distance D can be represented as a fuzzy set as:

Distance, D = Fuzzy Set [{BN, p}, {NN, q}, {WN, r}]

Where: p = the membership grade for Best Node in Distance calculation

q = The membership grade for Normal node in Distance calculation

r = The membership grade for Worst node in Distance calculation

The second parameter, power consumed P can be represented as a fuzzy set as:

Power consumed, P = Fuzzy Set[{BN, s}, {NN, t}, {WN, u}]

Where: s = The membership grade for Best Node in the calculation of power consumption

t = The membership grade for Normal node in the calculation of power consumption

u = The membership grade for Worst node in the calculation of power consumption

The third parameter, trust T can be represented as a fuzzy set as:

Trust, T = Fuzzy Set[{BN, v}, {NN, w}, {WN, x}]

Where: v = The membership grade for Best Node in trust calculation

w = The membership grade for Normal node in trust calculation

x = The membership grade for Worst node in trust calculation

The final decision is made on the basis of the output of the intersection of the equivalent members of the fuzzy sets of the three parameters; distance, power consumed and trust value.

TABLE I: FUZZY RULES

Distance d	Power Consumed P	Trust T	Result
Low	Low	High	Best
Low	High	High	Normal
High	Low	Low	Normal
Low	High	Low	Worst
High	High	Low	Worst
Low	Low	Low	Normal
High	High	High	Worst

Table 1 shows the conditions for decision making in fuzzy logic for inputs and its corresponding results. The Fig. 1 shows the block representation of the decision making in our fuzzy system.

Let distance, trust and power consumed be denoted by D, T and P:

- If D and P are less and if T is high then node is a best node.
- If D is less, P is high and T is high then node is a normal node.
- If D is high, P is less and T is less then node is a normal node.
- If D is less, P is less and T is less then node is a normal node.
- If D is less, P is high and T is less then node is a worst node.
- If D is high, P is less and T is less then node is a worst node.
- If D is high, P is high and T is high then node is a worst node.
- If D is high, P is high and T is less then node is a worst node.

The if-then rule simplifies this as the following.

Defuzzification of the fuzzified values can be carried out by more than a few techniques such as centroid average method, max centre method, mean of maxima, smallest of maximum and largest of maximum. In our case, we defuzzify using the maximum method. After decision making on the basis defuzzification, the normal and the best nodes are selected by the cluster head for data aggregation whereas the worst nodes are deserted by the cluster head. Then the cluster head transfers the aggregated data to the destination i.e., sink. Since the values of malicious and faulty sensors are not aggregated, secure data aggregation is ensured in the wireless sensor network.

IV. RESULTS AND DISCUSSION

The performance of our Fuzzy Based Secure Trust Aware Routing (FBTARF) technique is evaluated through NS2 Network Simulator. Table 2 summarizes the simulation parameters used.

TABLE II: SIMULATION PARAMETERS

No. of nodes	40
Area Size	1500 * 1500
Mac	802.11
Routing Protocol	DSDV
Simulation Time	20sec
Traffic Source	CBR
Packet Size	512 bytes
Rate	100-250 kb
Transmission Range	200 m
Transmission Power	0.400 W
Receiving Power	0.690 W
Initial Energy	5 joules

Misbehaving Nodes	3
Number of Clusters	5

A. *Performance Metrics*

The performance of FBTARF technique is compared with the normal TARF. The performance is evaluated mainly, according to the following metrics.

- **Average Packet Delivery Ratio:** It is the ratio of the number of packets received successfully and the total number of packets transmitted
- **Throughput:** It is the number of packets received by the sink successfully
- **Drop:** It refers to the no. of valid packets dropped due to malicious nodes
- **Energy:** It is the average energy consumed for the data transmission

B. *Performance Evaluation*

1). Packet Delivery Rate

The Simulation analysis shown in the below snapshot characterizes the Packets Data Ratio parameter in the FBTARF environments using the FBTARF protocol, TARF Protocol and the CTP Protocol. Packets Data Ratio is the ratio obtained based on the Packet Data Transmitted in the WSN Data flow during the simulation time of 10 seconds. The packets data rate parameter for FBTARF, TARF and CTP are compared in the Xgraph with Simulation Time in seconds as X-axis and Number of Packets ratio as Y-Axis. Thus in the FBTARF simulation analysis, the three protocol values are compared and the packets data ratio using the FBTARF protocol shows the better results.

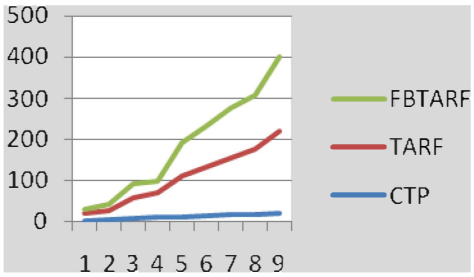

Fig. 2 Performance Analysis – Packet Delivery Rate

2). Throughput

The Simulation analysis shown in the below snapshot shows the Throughput Efficiency parameter in the FBTARF environments using the FBTARF, TARF protocol and the CTP Protocol. Throughput Efficiency is the overall successful data received rate. It is analyzed for the given protocol specification in the WSN Data flow during the simulation time of 10 seconds. The throughput efficiency for FBTARF,TARF and CTP are compared in the Xgraph with Simulation Time in seconds as X-axis and Number of Packets Ratio as Y-Axis. Thus in the WSN – TARF simulation analysis, the three protocol values are compared and the throughput efficiency using the FBTARF protocol shows the better results.

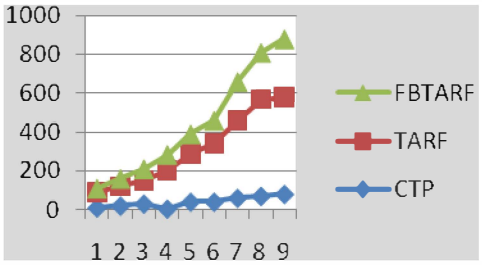

Fig. 3 Performance Analysis – Throughput

3). Energy

The Simulation analysis shown in the below snapshot characterizes the Total Energy Consumed in the FBTARF environments using the FBTARF,TARF protocol and the CTP Protocol. Total Energy Consumed is the overall energy used by the sensor nodes in the WSN Data flow during the simulation time of 20 seconds. The Total energy efficiency for FBTARF,TARF and CTP are compared in the Xgraph with Simulation resources in s as X-axis and Energy in Joules as Y-Axis. Thus in the FBTARF simulation analysis, the three protocol values are compared and the energy efficiency using the FBTARF protocol shows the better results.

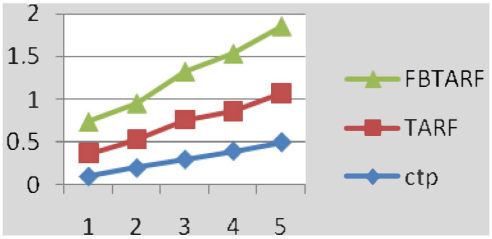

Fig. 4 Performance Analysis – Energy

V. CONCLUSION

To exploit the replay of routing information against harmful attackers and intruders, the proposed algorithm Fuzzy Based Trust-Aware Routing Framework (FBTARF) provides better security for WSN in multi-hop. For the survival of wireless sensor network under harsh and hostile environment, FBTARF provides trustworthiness and energy efficiency. With the concept of innovative trust management, FBTARF enables a node to keep track of the trustworthiness of its neighbours and there by select a reliable route path. Our main submissions are listed below.

1). Fuzzy based TARF effectively protects WSN from severe attacks through dynamic replaying routing information. Without time synchronization and known geographic information, fuzzification rules are formed based on dynamic mobility of the nodes

2). Extensive simulation and empirical analysis with large-scale WSN produces high resilience and scalability while using FBTARF and its proved by the graphical analysis

3). Finally, we demonstrate a proof-of-concept mobility based target detection application using trust, energy cost and distance estimators that are formulated on top of the Fuzzy based TARF.

The work can be extended in building a Fuzzy based TARF algorithm that takes not only Trust level and power level of each node but also the performance capacity of each node for efficiency improvement. The algorithm can be added to any existing routing algorithm for Trust and power management. The effectiveness of node can be easily found out by adding additional data aggregation about each node's capacity. Our Technique FBTARF is compared with multiple protocols like CTP and TARF to produce high throughput and PDR rate and less energy consumption.

REFERENCES

[1]. Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng - Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs - IEEE 2012 Transactions on Dependable and Secure Computing, Volume: 9 , Issue: 2

[2]. F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing Approach*. Morgan Kaufmann Publishers, 2004.

[3]. A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct 2002.

[4]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[5]. Al-Azawi, S., S. Boussakta and A. Yakovlev, 2012. Image compression algorithms using intensity based adaptive quantization coding. Am. J. Eng. Applied Sci., 4: 504-512. DOI: 10.3844/ajeassp.2011.504.512

[6]. Bhoopathy, V. and R.M.S. Parvathi, 2012. Energy constrained secure hierarchical data aggregation in wireless sensor networks. Am. J. Applied Sci., 9: 858-864. DOI: 10.3844/ajassp.2012.858.864

[7]. Ozdemir, S. and Y. Xiao, 2009. Secure data aggregation in wireless sensor networks: A comprehensive overview. Comput. Netw., 53: 2022-2037. DOI: 10.1016/j.comnet.2009.02.023

[8]. L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysis of mobile agent-based wireless sensor network," in *Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009)*, 20-24 2009, pp. 16 –19.

[9]. L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middleware for wireless sensor networks data fusion," in *Proceedings of Instrumentation and Measurement Technology Conference (I2MTC '09)*, 5-7 2009, pp. 378 –383.

[10]. W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based moving target methods in wireless sensor networks," in *IEEE International Symposium on Communications and Information Technology (ISCIT 2005)*, vol. 1, 12-14 2005, pp. 22 – 26.

[11]. J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in *Proceed- ings of the 10th International Conference on Advanced Communication Technology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 –78.

[12]. Jun, W., Z. Xin, X. Junyuan and M. Zhengkun, 2010. A distance-based clustering routing protocol in wireless sensor networks. Proceedings of the 12th IEEE International Conference on Communication Technology (ICCT), Nov. 11-14, IEEE Xplore Press, Nanjing, pp: 648-651. DOI: 10.1109/ICCT.2010.5688947

[13]. Feng, R., X. Xu, X. Zhou and J. Wan, 2011. A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory. Sensors, 11: 1345-1360. DOI: 10.3390/s110201345

[14]. Basaran, C., K.D. Kang and M.H. Suzer, 2010. Hop-byhop congestion control and load balancing in wireless sensor networks. Proceedings of the 35th IEEE Conference on Local Computer Networks (LCN), Oct. 10-14, IEEE Xplore, Denver, CO., pp: 448-455. DOI: 10.1109/LCN.2010.5735758

[15]. Almamani, I. and E. Almashakbeh, 2010. A powerefficient secure routing protocol for wireless sensor networks. WSEAS Trans. Comput., 9: 1042-1052.