Journal of Engineering and Applied Sciences 13 (6): 1326-1330, 2018
ISSN: 1816-949X
© Medwell Journals, 2018

Dynamic Trust Factor based Energy Efficient Relay Node Selection in HWSNs

[1]A.K. Velmurugan and [2]R. Jagadeesh Kannan
[1]Department of Computer Science and Engineering, St. Peter's University, Chennai, India
[2]School of Computing Science and Engineering, VIT University, Chennai, India

Abstract: The disseminated and shared environment of WSNs causes many challenges to offer security in network. A malevolent sensor node induces lot of packet losses, energy wastage and enhance in time to attain receiver. In this study, we investigate the dynamic trust factor based energy efficient relay node selection in heterogeneous WSNs. Here, the DTF calculation based on the node energy, average trust and hop count. This scheme used to increase both the network performance and lifetime in the network. The simulation results shows that the proposed scheme to increase the data received rate and reduce both the packet loss rate and energy utilization in the network.

Key words: Trust, energy, heterogeneous WSNs, proposed, utilization, lifetime

INTRODUCTION

Wireless Sensor Network (WSN) through sensor nodes support assembles and sends information about a supervised surrounding to a Base Station (BS). Security is of supreme anxiety for sensor network applications such as healthcare, battlefield surveillance, etc. Mostly, three main mechanisms that treat with security of network, prevention, detection and mitigation. However, it is very difficult to prevent WSNs from malevolent attacks, so, it is significant to identify them as early as probable. But execution of cryptography encryption techniques enhance the control overheads and also uses extra energy that is limited. A rising area of research to progress security is the execution of trust method that to diminish the hazard of usual security mechanism.

The capability to identify attacks and separating malevolent nodes can be enhanced achieved by trust-based mechanisms. Trust model get better security in open network surroundings based on a node's trust values computation and estimation for execution of a network security policy.

Literature review: A trust based Cluster Head (CH) collection mechanism (Anbuchelian *et al*., 2016) proposed to recover the security and lifetime of network. Firefly Algorithm (FA) treats combinational and numerical optimization multimodal problems capably. Efficient cluster based fault detection and recovery mechanism used to detect the fault and the subsequent recovery process. Trust-based Cluster head Validation and Outlier Detection Technique (TCVOD) (Sutaone *et al*., 2016) evaluated the malicious cluster-heads are detected and replaced. This scheme identified the false data, detect the outlier and consistency value of sensor node in the network. Enhanced Beta Trust Model (EBTM) (UmaRani *et al*., 2016) designed to find out malevolent attack in WSN. This recovery process is incorporated to progress the network throughput. Combining Trust and Expected Transmission Count (ETX) (Kantert *et al*., 2016) designed to develop the robustness of WSNs against untrustworthy nodes. Distributed Trust based Intrusion Detection (DTBID) approach (Dhakne and Chatur, 2015) developed the trust depend on some factors such as reliability, energy, data, etc. It constructs the trust based on direct trust, recommendation trust and indirect trust from these factors. This approach used to make a decision whether particular node is malicious node or not by intrusion detection technique.

An energy-aware trust derivation scheme (Duan *et al*., 2014) manages overhead while keeping sufficient security of WSNs. In this scheme, the game theoretic approach functional to the trust derivation procedure to diminish the overhead. Trust derivation scheme can attain both intended security and high efficiency. An Efficient Distributed Trust Model (EDTM) (Jiang *et al*., 2015) for WSNs according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. It improves the accuracy of recommendation trust. EDTM can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more effectively.

The trust management scheme (Ren *et al*., 2014) used to offer well-organized and vigorous trust data storage and trust generation for WSN. A geographic hash table to categorize storage nodes and to radically diminish

Corresponding Author: A.K. Velmurugan, Department of Computer Science and Engineering, St. Peter's University, Chennai, India

storage cost. We use subjective logic based consensus techniques to mitigate trust fluctuations caused by environmental factors. Adaptive Data-Communication Trust Mechanism (ADCT) (Talbi *et al*., 2015) used to effectively deal with compromise or malicious nodes. An adaptive purpose to estimate the direct trust between nodes also data trust manage with unreliable nodes in the data gathering despite their transmission capabilities. Random Sampling Consensus (RANSAC) (Wang *et al*., 2011) focused on the issue of sensing consistency in an acoustic target localization application. The reputation-based algorithm introduced to guarantee sensing consistency. The effectiveness and the efficiency of the algorithm are ensured by accurate estimation of the contamination ratio of node data. This method can successfully identify untrustworthy measurements and develop the localization performance.

An Energy Aware Sink Relocation (EASR) mechanism (Wang *et al*., 2014) uses information related to the residual battery energy of sensor nodes to adaptively adjust the transmission range of sensor nodes and the relocating scheme for the sink. Theoretical and numerical analyze are given to show that the EASR method can expand the network lifetime of the WSN significantly. The trust-based distributed topology management scheme (TRAST) (Mali and Misra, 2016) provides highest data received rate and transmission rate of the event in the presence of node replication attack. This scheme exploited the RSS values to estimate the trust rating with the assumption that RSS values. However, it cannot address the forged RSS values and scalability is an essential issue in this scheme.

MATERIALS AND METHODS

In this study, we design trust based relay node selection in HWSN. The trust evaluation estimate the node reliability of nodes and energy awake routing in the HWSN. The trust evaluation based on the node interaction, node data transmission, node suggestion trust in the HWSN. This trust method identifying the unreliable node and transmit the data through the trusted node in the WSNs.

This network consists of a super node and many sensor nodes spread within a limited field. Every sensor node knows its location by using localization technology and the super node knows all node's locations and it consist of additional amount of node coverage and energy. But the sensor node has a limited communication range. In this network, the sensor node collects the information from the environment and it transfer the data to BS through super node. Here, the super node acts as a relay node. If the BS is long distance, the super node transmits the information through multiple super nodes.

While data transmission, the sensor node chooses the relay node based on the dynamic trust factor. The dynamic trust factor computation as follows:

- Node trust
- Node interaction trust
- Node suggestion trust
- Comprehensive trust

Node trust: The node trust value evaluated based on the node Received Signal Strength (RSS). The node trust rate for node i to j is given as:

$$NT_{i\to j} = f(R, RSS_{i\to j}) \tag{1}$$

$$R = \frac{\delta}{\delta+\theta} \tag{2}$$

Where:
δ = Number of communication between node I to node J
θ = Integer constant

Node data trust: The node data trust represents the ratio of average successful forwarded packet to the average amount of forwarded packet in the network. Here, the node I communicate the node J at time t, the data trust computation is given as:

$$\frac{\vee_{I\to J}(t1)}{\wedge_{I\to J}(t1)}, \frac{\vee_{I\to J}(t2)}{\wedge_{I\to J}(t2)}, \ldots, \frac{\vee_{I\to J}(tn)}{\wedge_{I\to J}(tn)} \tag{3}$$

Where:
$\vee_{I\to J}(t1)$ = Successful data transmission rate
$\wedge_{I\to J}(tn)$ = Failure data transmission rate

The average data trust calculation is given as:

$$RT_j = \frac{\sum_{j=0}^{n} \frac{\vee_{I\to J}(t_i)}{\wedge_{I\to J}(t_i)}}{n} \tag{4}$$

here, n represents the number of interactions in the network.

Node suggestion trust: The node suggestion trust represents the neighbor node reports that node is reliable or unreliable. The suggestion trust of node I to K is given as:

$$N_{ST} = \partial_{i\to j} \times \partial_{j\to k} \tag{5}$$

Where:
i = Trust evaluator
j = Recommender of node i
k = End of evaluation

Comprehensive trust: The comprehensive trust is the total trust that combines the node trust, node suggestion trust and node data trust. The node of average trust calculation is given as:

$$\text{Avg.\_Trust} = \frac{\text{NT+NST+NDT}}{3} \quad (6)$$

Dynamic trust factor: The node dynamic trust factor is computed by average trust, node energy and hop count. The trust factor calculation is given as:

$$\text{DTF} = \mu\times\text{Avg\_Trust}+\nu\times\text{Energy}+\lambda\times\text{hop\_count} \quad (7)$$

Figure 1 indicates the flowchart of the proposed scheme. In this scheme, the sensor node transmit the data to base station through the super node in the HWSNs. Here, the super node acts as a relay node. The relay node is elected based on the Dynamic Trust Factor (DTF). The DTF is calculated by node trust, node suggestion trust and node data trust. The neighbor node DTF is greater than the threshold that node is elected as a relay node. This process is repeated until the source reaches the destination.

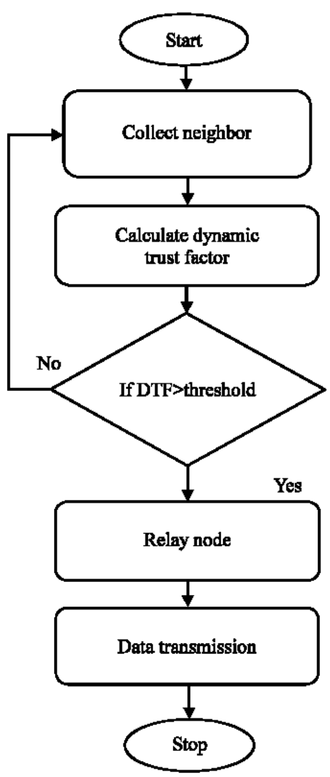

Fig. 1: Flow chart of the proposed scheme

RESULTS AND DISCUSSION

In this study, we analyze the simulation results of proposed method. The performance evaluation is done through the Network Simulator NS-2. In this simulation, 50 nodes randomly distributed within the network field of size 1200×1100 m.The parameters used for the simulation of the DTF-EER are tabulated in Table 1.

The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the PEAT is evaluated by the parameters packet delivery rate, packet loss rate, average delay, throughput and residual energy.

Packet delivery rate: Packet Delivery Rate (PDR) is the ratio of amount of data packets established to the amount of data packets sent by the source node. The PDR is calculated by the Eq. 8. Figure 2 reports that the amount of data packets received by the DTF-EER is larger than the TRAST:

$$\text{PDR} = \frac{\text{Total pack received}}{\text{Total pack send}} \quad (8)$$

Table 1: Simulation parameters of DTF-EER

Parameters	Values
Channel type	Wireless channel
Simulation time	50 sec
Number of nodes	50
MAC type	802.11
Traffic model	CBR
Simulation area	1000×1000
Transmission range	250 m
Network interface type	Wirelessphy

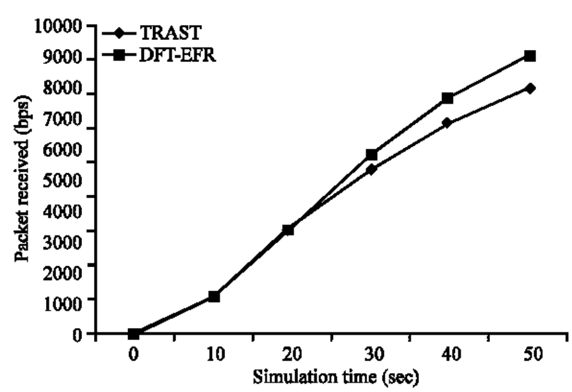

Fig. 2: Packet delivery rate of TRAST and DTF-EER

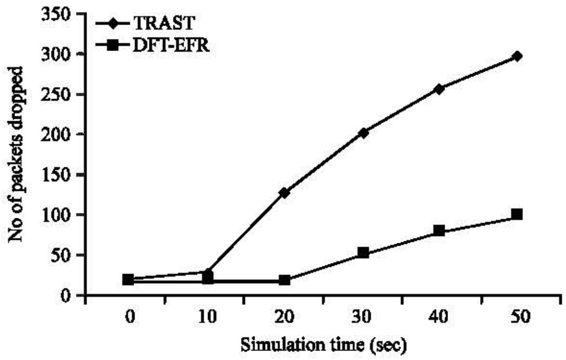

Fig. 3: Packet loss rate of TRAST and DTF-EER

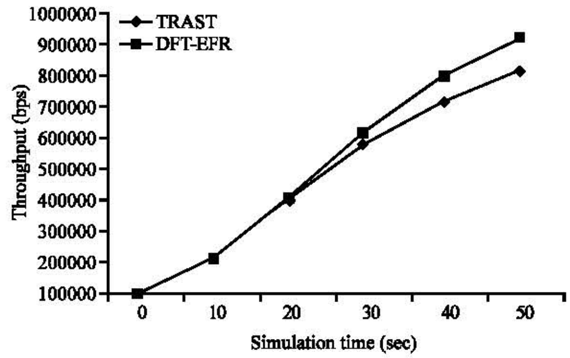

Fig. 5: Throughput of TRAST and DTF-EER

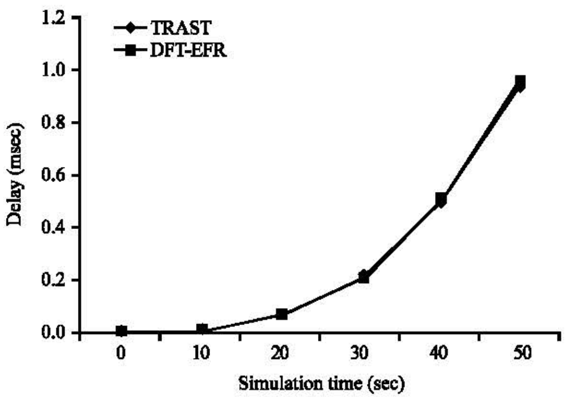

Fig. 4: Delay of PEAT and TAM

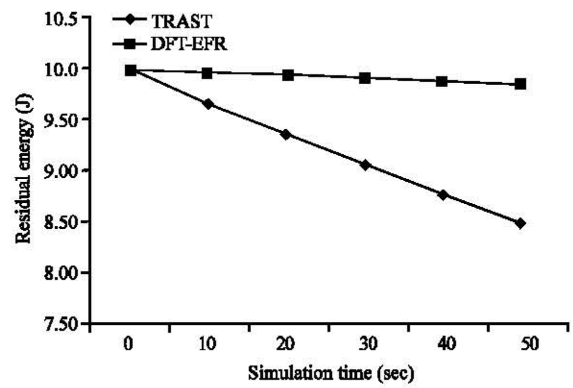

Fig. 6: Residual energy of TRAST and DTF-EER

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 PLR is calculated by Eq. 9:

$$\text{PLR} = \frac{\text{Total pack dropped}}{\text{Total pack send}} \tag{9}$$

Figure 3 shows the packet loss rate of the DTF-EER protocol is lesser than the TRAST. Lower packet loss rate obtains higher performance of the network.

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 Eq. 10:

$$\text{Average delay} = \frac{\text{Pack received time} - \text{Pack sent time}}{\text{Time}} \tag{10}$$

Figure 4 demonstrate that the delay of TRAST and DTF-EER. The average delay of the TRAST is larger than the DTF-EER indicating the improved performance of the DTF-EER protocol.

Throughput: Throughput is the average of successful messages delivered to the destination. The average throughput is calculated using Eq. 11:

$$\text{Throughput} = \frac{\sum_0^n \text{Pack received}(n)*\text{Pack size}}{1000} \tag{11}$$

Figure 5 shows the performance of throughput of PEAT and TAM protocols. The throughput of the TRAST is lesser than the DTF-EER. It represents increase the efficiency of the DTF-EER protocol in the network.

Residual energy: The amount of remaining energy present in a node at the current instance of time is said to be residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations.

Figure 6 shows that the residual energy of the network is better for the proposed scheme DTF-EER when compared with the existing scheme TRAST.

CONCLUSION

In this study, we introduced dynamic trust factor based energy efficient relay node selection in HWSNs. DTF-EER method used to identify the unreliable node and transmit the data through the trusted route in HWSN. The relay node selection based on the node energy, hop count and average trust. The simulation result demonstrates that the proposed scheme to reduce the unreliable node participating and increase the energy efficiency in the network.

REFERENCES

Anbuchelian, S., S. Lokesh and M. Baskaran, 2016. Improving security in wireless sensor network using trust and metaheuristic algorithms. Proceedings of the 3rd International Conference on Computer and Information Sciences (ICCOINS'16), August 15-17, 2016, IEEE, Kuala Lumpur, Malaysia, ISBN:978-1-5090-2550-3, pp: 233-241.

Dhakne, A.R. and P.N. Chatur, 2015. Distributed trust based intrusion detection approach in wireless sensor network. Proceedings of the Conference on Communication Control and Intelligent Systems (CCIS'15), November 7-8, 2015, IEEE, Mathura, India, ISBN:978-1-4673-7540-5, pp: 96-101.

Duan, J., D. Gao, D. Yang, C.H. Foh and H.H. Chen, 2014. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. IEEE. Internet Things J., 1: 58-69.

Jiang, J., G. Han, F. Wang, L. Shu and M. Guizani, 2015. An efficient distributed trust model for wireless sensor networks. IEEE. Trans. Parallel Distrib. Syst., 26: 1228-1237.

Kantert, J., F. Reinhard, G.V. Zengen, S. Tomforde and S. Weber *et al*., 2016. Combining trust and ETX to provide robust wireless sensor networks. Proceedings of the 29th International Conference on Architecture of Computing Systems (ARCS'16), April 4-7, 2016, VDE, Nuremberg, Germany, ISBN:978-3-8007-4157-1, pp: 1-7.

Mali, G. and S. Misra, 2016. TRAST: Trust-based distributed topology management for wireless multimedia sensor networks. IEEE. Trans. Comput., 65: 1978-1991.

Ren, Y., V.I. Zadorozhny, V.A. Oleshchuk and F.Y. Li, 2014. A novel approach to trust management in unattended wireless sensor networks. IEEE. Trans. Mobile Comput., 13: 1409-1423.

Sutaone, M., P. Mukherj and S. Paranjape, 2016. Trust-based cluster head validation and outlier detection technique for mobile wireless sensor networks. Proceedings of the 2016 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET'16), March 23-25, 2016, IEEE, Chennai, India, ISBN: 978-1-4673-9339-3, pp: 2066-2070.

Talbi, S., M. Koudil, A. Bouabdallah and K. Benatchba, 2015. Adaptive data-communication trust mechanism for clustered wireless sensor networks. Proceedings of the 2015 IEEE Conference on Global Communications (GLOBECOM'15), December 6-10, 2015, IEEE, San Diego, California, ISBN:978-1-4799-5952-5, pp: 1-6.

UmaRani, V., K.S. Sundaram and D. Jayashree, 2016. Enhanced beta trust model in wireless sensor networks. Proceedings of the 2016 International Conference on Information Communication and Embedded Systems (ICICES), February 25-26, 2016, IEEE, Chennai, India, ISBN:978-1-5090-2553-4, pp: 1-5.

Wang, C.F., J.D. Shih, B.H. Pan and T.Y. Wu, 2014. A network lifetime enhancement method for sink relocation and its analysis in wireless sensor networks. IEEE. Sensors J., 14: 1932-1943.

Wang, X., L. Ding and S. Wang, 2011. Trust evaluation sensing for wireless sensor networks. IEEE. Trans. Instrum. Meas., 60: 2088-2095.