Grenze International Journal of Engineering and Technology, Special Issue

E-TSRP: An Efficient Trust-based Secure Routing Protocol for Energy-Constrained WSNs

Tayyab Khan[1] and Karan Singh[2]
[1-2] School of Computer and Systems Sciences, JNU, New Delhi-110067, India
Email: tayyabkhan.cse2012@gmail.com, karancs12@gmail.com

***Abstract*—Due to unexpected (selfish) behavior and the dynamic nature of sensor nodes in the wireless sensor network, reliable and consistent data delivery has become a challenging as well as exigent task in sensor networks. Trust-based security schemes have been proved better than traditional cryptographic (authentication) schemes in terms of reduced cost, minimal overhead as well as a large number of selfish node detection.**

This paper presents a hybrid (centralized and distributed) trust model, which incorporates a multi-factor (trustworthiness of sensor nodes, residual energy, and hop count) routing strategy to determine the shortest as well as trusted routing path. This multi-factor strategy helps in selecting trusted nodes to forward data and minimize energy consumption due to shorter routing paths. The experimental outcome demonstrates the excellent performance of the proposed model (E-TSRP) in terms of robust trust score and average path length.

***Index Terms*— Trust, Routing, Energy Efficiency, Throughput, Delay.**

I. INTRODUCTION

A wireless sensor network (WSNs) incorporates several tiny sizes low-cost, resource restraint (memory, power, processor, bandwidth, as well as short communication range) ubiquitous sensor nodes (SNs or motes or stations). These ubiquitous SNs mostly deployed in the unattended (hostile, hazardous) environment to monitor events, collect continuous and discrete data, and sent (report or processed data) to the base station (sink node)[1-2]. Using this processed data; WSN plays a significant role in industrial controlling, home automation, smart cities, smart battlefield, etc. Moreover, WSNs are self-organized, low cost, limited bandwidth with a dynamic topology where SNs communicate via radio links [3-4].

Due to the distributed, Adhoc, dynamic, dense, and collaborative nature of Wireless sensor networks, SNs are vulnerable (prone) to failure, attacks (unexpected behaviors) that lead to unreliable communication. Once a SN is captured by any attack (adversary force), false data is injected and spread in the network to collapse the sensor network. When SN itself become selfish and try to misguide the network, cryptographic algorithms are not an efficient and wise solution since they are less reliable (not robust against internal threats) and impose high overhead. In such cases, trust-based security solutions are found reliable and valuable that computes the dependability and consistency of SNs for the endurance of WSN [6-8].

LEACH, EEHC, and EC [9-11] provide an excellent clustering scheme to enhance network measurability and throughput. Within a cluster, a cluster with a sufficient number of resources (CPU, power, memory) is elected as a cluster head (CH) that monitors the behavior of cluster (group) members and states the degree of trustworthiness. Th e CH identifies the malicious nodes within the cluster and selects the reliable route to

Grenze ID: 01.GIJET.6.2.505

transmit the data. The altered information about the trustworthy (genuine) SNs of the whole network is maintained in a database. The size of the database and size of the network are directly proportionally to each other. It is unfeasible for a particular SN to store, compute, and monitor the trust scores with alteration of the whole network.

Trust (in WSN or IoT) provides several advantages and resolve various severe issues such as access control, protection from internal attacks, etc., that cannot be solved using customary security solutions. Trust models distinguish genuine and malicious SNs by calculating their trust scores[1-5]. Trust concept plays a significant role in designing a robust, secure model as well as finding a trusted shortest routing path by eliminating faulty (less powerful, malicious) SNs. Trust improves node's collaboration for efficient routing of packets[9-12].

Routing (network layer responsibility) is a process to locate an optimal path from source (s) to the destination (d). The routing protocol is a procedure (method) to choose and maintain an appropriate path for the data to travel from source node to destination (sink) node. However, the routing process faces numerous difficulties during optimal (shortest and trustworthy) route selection, which depends upon network type, application type, channel characteristics, and other performance metrics. A proper routing protocol must consider the desires/demands of applications (quick data transfer, throughput, minimum interruption, delay). In small size WSN, SNs can communicate directly, but big WSNs (having large coverage area) require multi-hop communications since most of the SNs are not closer to the base station (BS). In multi-hop communication (sometimes referred as indirect communication [28]), SNs transmitted processed data to other SNs along with the information of a trusted path towards the sink. Multi-hop routing is susceptible to a range of internal attacks due to WSN's characteristics. These internal attacks affect the security and credibility of information and data generated by the SNs.

Designing an efficient routing protocol for WSNs is demanding as well as most challenging since SNs are dynamic (frequent changes in topology) and resource constraint nodes that generate redundant data. Removal of the redundant data is itself a challenging task since most of the time, All SNs monitor the same data and produce the same outcome. Moreover, the continuous flow of non-redundant data is also necessary for the better performance of WSN. Due to the aforementioned concern, there are various routings protocol design issues such as energy efficiency, security, scalability, complexity, robustness, delay, connectivity, coverage, sensor location, and transmission models. Several states of the art routing protocols have been developed to remove aforesaid limitations that employ familiar routing tactics, e.g., clustering, data aggregation, data-centric methods, in-network processing as well as different role assigned to SNs.

This paper presents a trust-aware approach for achieving secure routing in WSNs with minimal routing and network overhead during multi-hop information transmission. An interesting trust function is employed to evaluate the trust score of SNs based on their cooperative behavior. These trust values, along with hop count and energy threshold, assist in finding the reliable routing path.

II. Literature Review

This section discussed the existing work related to various trust models as well as trust aware routing protocols for WSNs.

Riaz Ahmed Shaikh, et al. [13] discussed on group-depended TMS (GTMS) for clustered wireless sensor networks. The author states that existing TMS for wired and wireless ad hoc networks are not suitable for sensor networks due to higher consumption of resources like memory and power.

Alexander et al. [14] wrote on the trust-based methodology of countering attacks for wireless sensor networks, which employs Bayes' theorem and normal distribution.

Kaur et al. [15] present "A Review of Various Scheduling Techniques Considering Energy Efficiency in WSN." The author states that job (task, resources) scheduling plays a vital role in allocating limited resources wisely in WSN to reduce resource (energy, storage) consumption and provide a comparative analysis of various energy-efficient scheduling algorithms. Among the various techniques mentioned in this work, Task scheduling seems to be better in terms of average turnaround time and waiting time.

Zhou et al. [16] proposed, "A three-phase energy-balanced heuristic for mobile sink scheduling in hybrid WSNs." The whole network is divided into equal size clusters containing grid cells based on a k-dimensional tree algorithm to reduce the energy consumption in order to prolong the network lifetime. Data collected with the help of mobile sink from the cluster heads are routed using the traveling salesman problem (TSP). Experimental results exhibit the remarkable performance in terms of consumption of balanced energy (for sink mobility and data gathering) in each cluster and optimal division of grid cell into clusters.

Azharuddin et al.[17] proposed a distributed algorithm known as DFTR for energy conservation and fault tolerance (in case of cluster heads (CHs) failure) in wireless sensor networks for their development and survival. DFTR selects an intermediary relay node by using a cost function during routing and provides a fault-tolerant method by selecting next-hop CHs if cluster heads (CHs) gets failed. Simulation results using Weibull distribution under various scenarios exhibit the usefulness, effectiveness, and efficiency in terms of numerous metrics like energy consumption, dead CHs, packet delay, and throughput. One negative point of this approach is the static scenario, not considering the partial and transparent failure of the CHs.

Wang et al. [18] proposed an efficient shortest path based mechanism with the help of Aware Sink Relocation (EASR) to diminish the energy consumption of SNs, traffic loads along with space and message cost in order to enhance the performance and lifetime of WSN. It is advantageous because, in the case of an adequate amount of energy lost by the cluster head, the sink can be relocated, and malicious nodes are dropped out. Simulation results demonstrate high performance in terms of throughput. Communication overhead trusted routes and mobility are the research gaps in this work.

Zahariadis et al. [19] proposed a trust aware security model to detect and protect against malicious behavior of SNs. The proposed method uses location information, direct and indirect trust to make the final routing decision. The author states that the proposed solution is scalable and attack resilient. However, the authors analyze the design and implementation cost, validation process.

adnan et al. [20] resolve the limitations of existing routing protocols (TERP) that employ the trust concept for secure routing. TERP incurs less energy consumption along with reduced overhead due to the distributed trust model. TERP effectively identify unexpected behavior and incorporate composite function for reliable routing decisions.

Beheshtiasl et al. [21] proposed a trusted routing protocol based on the fuzzy logic concept. The author states that trusted routing improves throughput as well as the lifetime of WSNs. The proposed method reduces energy consumption and obtains robust trust values using fuzzy logic to identify the secure and non-link breakable route.

Yang et al. [22] discussed a trust evaluation based secure routing scheme (EOSR) for WSNs to isolate faulty SNs from the routing path. EOSR effectively counter internal routing threats and optimizes energy. EOSR uses communication trust, hop count, and residual energy to find reliable as well as the shortest routing path.

Kalidoss et al. [23] proposed a trusted multi-hop routing scheme for WSNs that employs Quality of service, an authentication scheme, and overall trust score to improve security as well as reliability of transmitted data. In addition, CHs are selected based on the trust score and QoS parameter. The proposed routing scheme is better than existing ones in terms of delay and energy consumption since it uses path trust, energy trust, and hops count before making the final decision.

Rajaram et al. [24] proposed a shortest path trustworthy routing scheme that employs a link-state routing protocol and indirect trust to counter various internal threats like selective forwarding, wormhole, and sinkhole. The author believes data faulty (unreliable) SNs in WSN primarily influence the performance of the network. In the projected routing approach, if any routes fail anytime, immediately another trusted route is founded by the SRPT algorithm. However, the authors have not discussed the convergence rate and energy efficiency and overhead issues.

Balaji et al. [25] proposed SAR-RG scheme to mitigate DOS attacks as well as improve cooperation among SNs. SAR-RG is a game theory-oriented scheme that employs trigger methodology, punishment concept to diminish the effect of malicious SNs in MANET.

Duan et al. [26] proposed a secure routing framework TSRF that meets the security requirements to hindrance various malicious behaviors. TSRF employs QoS metrics along with trust (computation, derivation) metrics to achieve acceptable efficiency as well as security for dense sensor networks. Moreover, TSRF uses semirings theory and analyzes the impact of different internal attacks on the performance of routing.

Qin et al.[27] projected a secure routing mechanism known as TSSRM to resist numerous collective unexpected behavior as well as reduce overheads. In addition, TSSRM analyzes the impact of malicious behavior on WSN in terms of efficiency, throughput, etc. and optimizes a trustworthy route selection algorithm by considering QoS, trust parameters to improve the effectiveness of WSNs.

III. MOTIVATION

In recent years, Trust aware routing protocols have become attractive tools for the research community since they improve resource efficiency, dependability, and isolating faulty nodes among SNs during routing to prolong the network lifetime (efficiency). However, most of the existing trust-based routing schemes [21-27] do not focus on fundamental issues such as throughput, frequent routes breakages, route stability, congestion, energy consumption, delay, Quality of service (QoS), etc. and hence incapable of ensuring security during multi-hop communication. To remove the aforementioned limitations from the existing trust-based routing protocols [20,22,23,25], we have proposed a trust-based secure routing protocol that employs a multi-factor (trustworthiness of sensor nodes, residual energy, and hop count) routing strategy to determine shortest as well as trusted routing path.

IV. Proposed Work

This section presents a description of the proposed work with goals and underlying assumptions. Our main goals are to improve reliability (trustworthiness) efficiency, throughput, and energy efficiency, scalability, path length, as well as load balancing in a harsh and congested environment.

Assumptions

i) Source node and sink node are highly trustworthy, i.e. (not faulty or malicious at any point of time)
ii) Sensor nodes (SNs) are homogeneous in respect of all parameters
iii) Network is static with clustered topology. Trust-based clustering [29] is employed to divide the whole network into clusters. CH is responsible for data aggregation as well as forwarding it from CH to CH.
iv) Each SNs monitors the activities of 1-hop neighbors through the learning unit. Activities may be packet forwarding behavior, processing, etc
v) Selfish node can drop any number of packets. Moreover, it sends a false route replies to become an advisable (reasonable) node for routing traffic.
vi) Trust domain : [0 4] and trust threshold (θ) =2
vii) Timing window [30] is employed to record the cooperative and non- cooperative interactions.

The proposed work provides a novel trust function to evaluate the trust score of the individual SNs and route setup algorithm to discover the most reliable (energy aware, trusted) route. Incorporation of trusted, as well as energy-aware SNs during routing, improves the reliability, throughput, etc. Moreover, during trust score computation, we employ direct trust, aggregate indirect trust, and energy trust as well as the expected probability of the behavior. Figure 1 represents the flow diagram of E-TSRP.

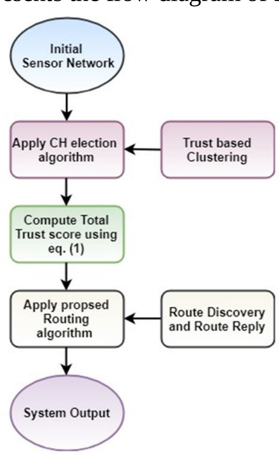

Figure 1. Flow diagram of E-TSRP

The total trust score of node x has for node y during Δt time is defined by $T_{x,y}(\Delta t)$ using (1) as follows

$$T_{x,y}(\Delta t) = w_1 * DT_{x,y}(\Delta t) + w_2 * AIT_{X,Y}^{k}((\Delta t) + w_3 * ET(\Delta t) + w_4 * 4 * Ep_{x,y}(\Delta t) \tag{1}$$

Where $DT_{x,y}(\Delta t)$ is a direct trust evaluator function that is defined as follows where

$$\mathbf{DT_{x,y}(\Delta t)} = \left[4 \times \left(\frac{S_{x,y}^{C}(\Delta t)+1}{(S_{x,y}^{C}(\Delta t)+U_{x,y}^{C}(\Delta t)+2))} \right) * \frac{1}{\sqrt[2]{\eta * (U_{x,y}^{C}(\Delta t)+1)}} * \left(\frac{S_{x,y}^{C}(\Delta t)}{S_{x,y}^{C}(\Delta t)+1} \right)^{\alpha} \right] \tag{2}$$

The term α and η are adjustable parameters used to provide incentive and penalty as per the need of the application. The first term $\left(\frac{S_{x,y}^{C}(\Delta t)+1}{(S_{x,y}^{C}(\Delta t)+U_{x,y}^{C}(\Delta t)+2))}\right)$ indicate the ratio of cooperative (successful) interactions to the total interactions in (Δt) time. The second terms $\frac{1}{\sqrt[2]{\eta*(U_{x,y}^{C}(\Delta t)+1)}}$ gives flexible penalty with the rise in non- cooperative interactions and third term $\left(\frac{S_{x,y}^{C}(\Delta t)}{S_{x,y}^{C}(\Delta t)+1}\right)^{\alpha}$ gives incentive with the gradual rise in cooperative interactions. The multiplicative factor 4 is used to make trust values within the specified range. In the proposed (1), the sum of weights is 1. Fig. 2 indicates the trust evaluation component.

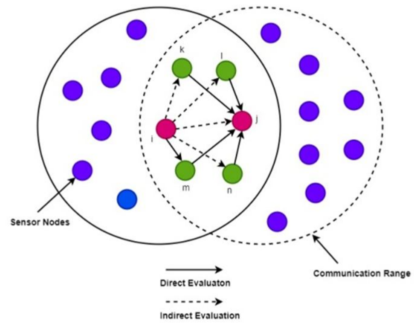

Figure 2. Component of Trust Calculation

The aggregate indirect trust $\mathrm{AIT}_{X,Y}^{k}((\Delta t)$ is computed using (3) as follows

$$\mathrm{AIT}_{X,Y}^{k}((\Delta t) = \frac{\sum_{k \neq x, k \in N_j} DT_{x,k}(\Delta t) * DT_{k,y}(\Delta t)}{N_j} \quad (3)$$

Where N_j represent the number of direct trusted neighbors of node x that assist in computing indirect trust scores. Indirect trust calculation using this approach brings various advantages such as identify and segregate faulty SNs as early as possible. Another benefit is accelerating the trust evaluation convergence rate as well as prevents false recommendations.

The energy trust of a SN x at (Δt) time($ET^{x}(\Delta t)$) is computed with the help of predefined threshold value E_{th} which is 20% of the total energy. If the current energy level (CEL) of a SN (let's say x) is greater than 50% of total energy, then SN x is highly trusted. If 20% of total energy < $\mathrm{CEL}^{x} \leq$ 50% of total energy, then SN x is trusted else it is non-trusted.

The expected positive probability $\mathrm{Ep}_{x,y}(\Delta t)$ of local SNs has been considered to improve the robustness as well as address uncertainty problem. The $\mathrm{Ep}_{x,y}(\Delta t)$ predicts the future activities (behavior) of SNs with the help of beta probability density function (BPDF). [20] States that the uncertainty issue of trust modeling problem can be rationally resolve using BPDF. Suppose $G_{x,y}$ & $B_{x,y}$ are defined as the good and bad behave respectively of SN y observed at SN x on the basis of the packet forwarding ratio, then $\mathrm{Ep}_{x,y}(\Delta t)$ can be defined using (4) as follows

$$\mathrm{Ep}_{x,y}(\Delta t) = \frac{G_{x,y}+1}{(G_{x,y}+1)+(B_{x,y}+1)} \quad (4)$$

Where $G_{x,y}$ and $B_{x,y} \geq 0$. Final trust value $T_{x,y}(\Delta t)$ using (1) gives the global trust values to SNs. SNs having trust score >2 are qualified as trusted nodes that can be participated in routing. SNs having trust score ≤ 2 are considered as non-reliable SNs that should not be participated in the routing process.

V. Route setup mechanism (RSM)

The route setup mechanism (RSM) is responsible for finding the trusted (reliable) route. In this work, we have extended the routing mechanism of the well-known AODV protocol by incorporating the energy-aware trust concept. The proposed approach reduces additional overheads as well as improves throughput by incorporating energy and trust score information into the RREQ and RREP packets. We defined the routing cost (RC) of path consist of reliable SNs i,j,k…n ∈ V using (5) where V represents a set of SNs.

$$RC = \alpha * T_{x,y}(\Delta t) + \beta * \text{hop count} + \gamma * \text{Residual Energy} \quad (5)$$

The advantage of RSM over [20-27] is that here, trust value is more robust since final trust value itself incorporates energy trust. Moreover, during the routing process, we compute route cost, which employs residual energy concept whenever discovering any new route.

Algorithm: Routing discovery process (Routing Request and route reply)

During the route discovery process, the source node (say s) broadcasts an RREQ frame to next-level (neighbors) nodes. Based on the residual energy level and trust score of SNs, either the RREQ frame is dropped by next level SNs or the RREP frame is dropped. Algorithm 1 explained this route request process in a detailed manner.

Algorithm 1: Routing discovery process (Routing Request)

Input: set of sensor nodes, Energy threshold(Th_{energy}), RREQ, RREP, time to live (TTL), current node (n_{curr}), previous node (n_{prev}), final trust values of sensor nodes ($T_{x,y}(\Delta t)$), trust threshold (θ)

Output: Route discover, start routing reply process

Step 1) initialize RREQ frame, current node, previous node

Step 2)

```
while (RREQ_TTL>0)
        Broadcast RREQ frames to downstream nodes
          n_prev = n_curr
            n_curr = current node
        if ( T_x,y(Δt)  ≥  θ & residual energy of current node < Th_energy)
                Drop RREQ frame by current node
                Break
        Else if ( T_x,y(Δt)  ≤  θ & residual energy of current node ≥ Th_energy)
                Discard RREP frame by precursor node
             END if
        If ( current node = = destination node)
                Start routing reply process and return
        END if
          RREP_TTL = RREP_TTL -1
END while
```

Once RREQ reached to the destination node (d), it unicast RREP packet to s along with the reverse route entry made by each intermediate SN at the time of broadcasting RREQ by the source node. Every intermediate SNs ensure the trustworthiness of the RREP packet coming from downstream nodes by analyzing the trust score contained in the route reply packet (RREP). The same process is repeated multiple times until RREP reaches the source node (s). Using this approach, we can eliminate non-reliable nodes (having a trust score < trust threshold) by drooping their RREP from the route selection. Hence, the source can find a suitable (trustworthy and energy-efficient) path among the available paths. Note that RREQ makes reverse route entry, and RREP makes forward route entry in neighbor nodes. At the end of this process, the source node determines the shortest, reliable as well as energy-efficient path.

VI. Simulations And Experimental Results

In this section, we discuss the effectiveness of the proposed scheme E-TSRP using Matlab (R2016a) in terms of trust value severity, average path length. Parameters values are taken in the proportion of [20] to provide better comparative results. Fig. 3shows the increment in the trust score of SNs with the increment in cooperative interactions. Moreover, E-TSRP provides flexibility through parameters (α and η) to tune the trust scores as per the actual application requirement.

Fig. 4 shows the comparative average path length for a packet to reach the destination node under a varying range of sensor nodes. E-TSRP uses RC function to achieve shorter paths. However, proposed may take a longer route for any packet if an available shorter route is not reliable (trustworthy, energy-efficient).

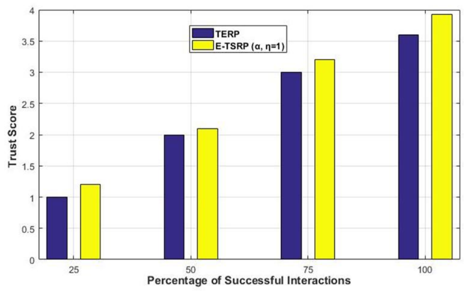

Figure 3. Change in trust score w.r.t successful interactions

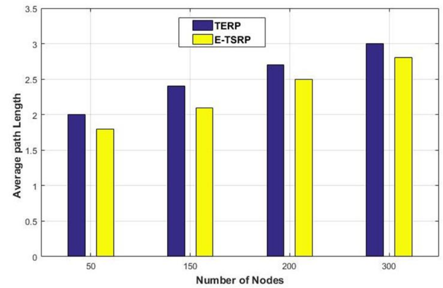

Figure 4. Average path length

VII. Conclusion & Future Work

In this paper, we propose an efficient Trust-based secure model (E-TSRP) to detect and alleviate various internal threats (adversely affect) by estimating the trust scores of sensors nodes in a quantitative way. E-TSRP is a multifactor routing approach that employs trust scores of nodes, residual energy, and path length to provide reliable routing paths among trusted nodes with reduced energy consumption. The experimental outcome shows better performance in terms of robust trust values and average path length. In the future, we are willing to extend this work for better route reply process by incorporating an efficient route maintenance process to analyze the network lifetime (in secs), average energy consumption (in joule), throughput (kbps) as well as average path length under varying network load.

Conflicts Of Interest

The authors declare that they have no competing interests.

Acknowledgments

This work was carried out in Secure and Computing laboratory, SC&SS, JNU, New Delhi, India, and sponsored by the project entitled “Development of Intelligent Device for Security Enhancement (iEYE)” with sanction order: DST/TDT/DDP12/2017-G.

References

[1] Yi Ren, Vladimir I. Zadorozhny, Vladimir A. Oleshchuk, and Frank Y. Li, "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 7, JULY 2014.

[2] Renjian Feng, Xiaofeng Xu, Xiang Zhou, and Jiangwen Wan "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory" *Sensors* 2011.

[3] Yanli Yu a,b, KeqiuLi a,, WanleiZhou b, PingLi b "Trust mechanisms in wireless sensor networks : Attack analysis and countermeasures" *ELSEVIER*, 2011.

[4] Farruh Ishmanov , Sung Won Kim, and Seung Yeob Nam"A Robust Trust Establishment Scheme for Wireless Sensor Networks" *Sensors,* 2015.

[5] Moutushi Singh, Abdur Rahaman Sardar, Koushik Majumder & Subir Kumar Sarkar "A Lightweight Trust Mechanism and Overhead Analysis for Clustered WSN" *IETE JOURNAL OF RESEARCH*, 2017.

[6] Singh, Santar Pal, and S. C. Sharma. "A survey on cluster-based routing protocols in wireless sensor networks." *Procedia computer science* 45,pp. 687-695,2015.

[7] Liu, Xuxun. "A survey on clustering routing protocols in wireless sensor networks." *Sensors*, Vol..12, no. 8,pp. 11113-11153, 2012.

[8] Boyinbode, Olutayo, Hanh Le, Audrey Mbogho, Makoto Takizawa, and Ravi Poliah. "A survey on clustering algorithms for wireless sensor networks." In *2010 13th International Conference on network-based information systems*, pp. 358-364. IEEE, 2010.

[9] Xiaoyong Li, Feng Zhou, and Junping Du "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks” *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 8, NO. 6, JUNE 2013.

[10] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V. Vasilakos "ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks" *IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE*, VOL. 16, NO. 4, JULY 2012.

[11] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT*, VOL. 9, NO. 2, JUNE 2012.
[12] Junqi Duan, Yajuan Qin, Sidong Zhang, Tao Zheng, Hongke Zhang "Issues of Trust Management for Mobile Wireless Sensor Networks" *IEEE* 2011.
[13] Shaikh, Riaz Ahmed, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee, and 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] Alexander,ElenaBasan,OlegMakarevich,"Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust" International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2016
[15] Kaur, Rajwinder, and Sandeep Sharma. "A Review of Various Scheduling Techniques Considering Energy Efficiency in WSN." *International Journal of Computer Applications*, ol.162, No.8, 2017.
[16] Zhou, ZhangBing, et al. "An energy-balanced heuristic for mobile sink scheduling in hybrid WSNs." *IEEE Transactions on Industrial Informatics*, Vol.12, No. ,pp. 28-40, 2016.
[17] Azharuddin, Md, and Prasanta K. Jana. "A distributed algorithm for energy-efficient and fault-tolerant routing in wireless sensor networks." *Wireless Networks*, Vol 21, No.1, pp. 251-267, 2015.
[18] Wang, Chu-Fu, et al. "A network lifetime enhancement method for sink relocation and its analysis in wireless sensor networks." *IEEE sensors journal*, Vol.14, No. 6, pp. 1932-1943, 2014.
[19] Zahariadis, Theodore, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas, Ioannis Papaefstathiou, Charalambos Vangelatos, and Lionel Besson. "Design and implementation of a trust-aware routing protocol for large WSNs." *International Journal of Network Security & Its Applications (IJNSA)* 2, no. 3, pp.52-68, 2010.
[20] Ahmed, Adnan, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan. "A trust aware routing protocol for energy-constrained wireless sensor network." *Telecommunication Systems*, Vol. 61, no. 1, pp. 123-140, 2016.
[21] Beheshtiasl, Azam, and Ali Ghaffari. "Secure and Trust-Aware Routing Scheme in Wireless Sensor Networks." *Wireless Personal Communications, pp.* 1-16, 2019.
[22] Yang, Tao, Xu Xiangyang, Li Peng, Li Tonghui, and Pan Leina. "A secure routing of wireless sensor networks based on trust evaluation model." *Procedia computer science* 131, pp. 1156-1163, 2018.
[23] Kalidoss, Thangaramya, Logambigai Rajasekaran, Kulothungan Kanagasabai, Ganapathy Sannasi, and Arputharaj Kannan. "QoS Aware Trust-Based Routing Algorithm for Wireless Sensor Networks." *Wireless Personal Communications*, pp. 1-22, 2019.
[24] Rajaram, S., A. Babu Karuppiah, and K. Vinoth Kumar. "Secure routing path using trust values for wireless sensor networks." *arXiv preprint arXiv*, pp. 1407.1972 , 2014.
[25] Balaji, Subramanian, Eanoch Golden Julie, Yesudhas Harold Robinson, Raghvendra Kumar, and Pham Huy Thong. "Design of a security-aware routing scheme in Mobile Ad-hoc Network using Repeated Game Model." *Computer Standards & Interfaces*, pp. 103358, 2019.
[26] Duan, Junqi, Dong Yang, Haoqing Zhu, Sidong Zhang, and Jing Zhao. "TSRF: A trust-aware secure routing framework in wireless sensor networks." *International Journal of Distributed Sensor Networks* Vol.10, no. 1, pp. 209436 ,2014.
[27] Qin, Danyang, Songxiang Yang, Shuang Jia, Yan Zhang, Jingya Ma, and Qun Ding. "Research on trust sensing-based secure routing mechanism for wireless sensor network." *IEEE Access*, Vol. 5, pp. 9599-9609, 2017.
[28] Shabbir, Noman, and Syed Rizwan Hassan. "Routing Protocols for Wireless Sensor Networks (WSNs)." Wireless Sensor Networks: Insights and Innovation, p.21,2017.
[29] Crosby, Garth V., Niki Pissinou, and James Gadze. "A framework for trust-based cluster head election in wireless sensor networks." In Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, IEEE, pp. 10,2006.
[30] Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks." *IEEE Access*, Vol.7, pp. 58221-58240,2019.