IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TBSK: TRUST BASED SECURE KEY SHARING SCHEME FOR HIERARCHICAL WSN TO DETECT MALICIOUS ACTIVITIES

[1]Dr. Lata B T, [2]Dr. Venugopal K R

[1]Assistant Professor, [2]Vice Chancellor

[1]Department of Computer Science and Engineering, UVCE, BU, Bengaluru

[2]Bangalore University, Bengaluru, India

Abstract: Trust based schemes have become vital role in providing security and reliability for various applications of Wireless Sensor Networks (WSN). Due to open environment sensor networks are vulnerable to attackers while routing data which degrade QoS. To overcome this problem, we propose Trust Based Secure Key Sharing scheme (TBSK) for cluster based WSN. In this scheme the network is partitioned into clusters and data transmission from Cluster Head (CH) to Base Station (BS) via inter-cluster is done by sharing lightweight secret keys. TBSK analyses dynamic trust degree value of single hop nodes on recommendation and experience to identify malicious nodes within the cluster. The goal is to ensure reliable data transmission and mitigate malicious node that exhibits malicious activities by dropping packets. The simulation experiment is carried on NS2 and performance results are analyzed in terms of packet delivery ratio, throughput, average end-to end delay and communication overhead.

Index Terms **- Cluster Head, Malicious, Security, Trust, Secret keys, Lightweight.**

I. INTRODUCTION

Sensor nodes are tiny lightweight, resource constrained and battery operated embedded devices which can self organize itself to form Wireless Sensor Network (WSN). Sensor nodes are deployed uniformly or randomly in an event monitoring area. These nodes continuously collect data from physical environment and reports to data collection node known as Base Station (BS) or sink [1-3]. However due to deployment nature, sensor nodes are susceptible to malicious attackers. Once the node is compromised, it misbehaves with other nodes by giving false feedback, disturbs normal network functions and misguides routes which lead to packet drop. To enhance network security, various cryptography authentication techniques have been proposed by researchers [4-7]. However cryptographic techniques cannot alone tackle and prevent attacks by adversaries. Thus we require robust trust based schemes to evaluate trust degree of node by analysing its behaviour and estimate node dependability and trustworthiness to mitigate malicious node [8-11].

Hierarchal clustering methods [12-16] improves network throughput, scalability and extends network lifetime compare to flat networks. In cluster network, Cluster Head (CH) is elected on high residual energy and it is responsible to collect data from sensor, aggregate and forward to BS, also CH detects malicious node which gives false recommendation about neighbour nodes.

WSN are resource constrained, fundamental requirements like resource efficiency and dependability have not received much attention in existing trust management schemes [10] [24] [25]. Existing clustered based trust schemes makes unrealistic for large scale and faces limitation such as computation overhead, memory overhead and energy. Furthermore, most of the existing trust scheme does not offer tolerable security measures and existing cryptographic functions are more complex and increases computational overhead. Existing approaches does not provide security while routing data. Thus impact of proposed solution **motivates** to make lightweight process for secure data routing and mitigate malicious activities. Main **contributions** in this paper include:

- Lightweight secret key sharing using XOR for secure routing through inter-cluster communication via CH and defending against data threats. Lightweight secret key requires less computation power and overhead compared to other key exchange techniques.
- Provide trust estimation among Cluster Members (CM) and cluster head (CH) by evaluating dynamic trust degree at CH, which also helps in detecting internal and external attacks.
- Trust values provides reliable decision making and reduces communication overhead through CH cooperation.

The rest of this paper is **organized** as follows. Section III describes the related works done. Section IV describes the proposed network model. In section V describes proposed trust scheme. In section VI the performance analysis and relative simulation are conducted. Finally, we draw the conclusion on the proposed scheme in section VII.

II. RELATED WORKS

In [17] author proposed trust management scheme for Healthcare-oriented Wireless Sensor Network (HWSN) to detect internal attacks and resolve security issues. This scheme uses binomial distribution to detect attacks like on-off and bad mouthing also has higher rate of detection and accuracy. This scheme is not scalable for large scale HWSN, but can effectively detect attacks in small scale HWSN. In [18] proposed direct and indirect trust evaluation scheme to improve security and mitigate cyber security attacks for cluster based WSN. In this scheme aggregates trust value history and eliminates several attacks based on bad recommendation. In [19] proposed trust management scheme for scalable WSN to detect and avoid malicious attacks. Time lapse function on forgetting curve is computed to evaluate direct trust and reputation function for indirect trust computation. Predefined threshold value is set to differentiate legitimate or selfish nodes. But this scheme has more communication overhead and does not give proper data report.

In [20] author proposed intrusion detection system based on protocol layer to secure WSN from security threats. Attacks are detected at each layer and trust value are evaluated by trust value deviation w.r.t. attack and trustworthiness of each layer (physical, MAC and network layer) are considered for evaluating trust metrics by taking aggregated trust value in each layer with predefined threshold value. This scheme can detect sinkhole, jamming and back-off manipulation attacks. In [21] proposed energy efficient clustering scheme to extend network lifetime. Hierarchical cluster network solutions improve scalability, network lifetime and communication overhead. Due to open media network are prone to security threats and in cluster process it becomes difficult to detect malicious activity since cluster head has to perform various tasks and tends to become more overhead with abundant traffic. This scheme discovers secure and reliable end to end path by detecting malicious node. However, it is observed that existing related works have more computation overhead due to cryptographic functions and does not react to different behaviour of malicious activities in the network.

III. NETWORK MODEL

Network consists of hierarchical WSN cluster and BS or sink shown in Figure 1. Network is partitioned into clusters. In each cluster, CH is selected on high residual energy and members (CM) communicates to CH through inter and intra cluster communication. CH is responsible to collect and forward aggregate data from CM to BS.

Assumptions

- Network is partitioned and clusters formation is done using clustering method [22] and cluster head is elected using [23] and trust computation and decision making is done by CH. BS assigns initial trust value to sensors and it is assumed that all the nodes are non-malicious initially.
- Secure key management scheme [15] is established for secure communication between nodes.
- Dynamic trust degree computation and the trust values for successful and unsuccessful transmission are assigned in range (0.5-1).
- BS has more resource and not compromised by attackers and monitors entire network.

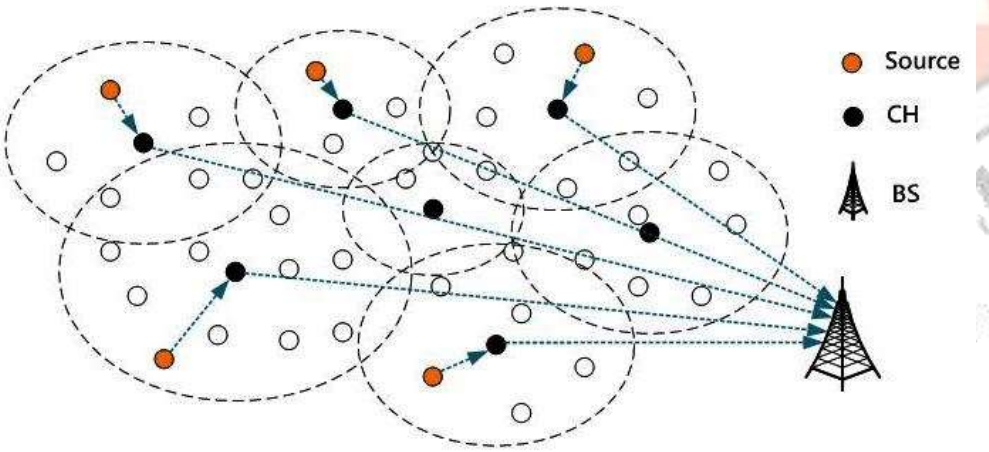

Figure 1: Hierarchical Network

IV. PROPOSED TBSK SCHEME

Key Gen Algorithm Phase using XOR

Input: Unique ID and Secret key
Output: Secret key is verified and establishment of trust recommendation

For each node a unique ID is assigned by BS is employed by using modified SHA-1

$N_{ID} = ((K' + 1) \oplus R_{Numb} \parallel H\left((K' + 1) \oplus ID \parallel R_{Numb}\right))$

where K' key generated using hash function and ID is unique identification of sensor node. R_{Numb} is random number initiated by BS. Secure key sharing coordination scheme for inter and intra cluster transmission is given as:

Step 1: BS generates unique id for nodes and n random secret keys $(S_{n1}, S_{n2} \dots \dots S_n)$ and forwards it to corresponding CH.
Step 2: Data D from corresponding cluster C_n is encrypted with cluster secret key $S_n$by performing XOR operation and is given as:

$$E_n = S_n \oplus D$$

Step 3: Encrypted data E_n of corresponding cluster is forwarded to the next cluster C_{n-1}through inter-cluster communication.
Step 4: Upon receiving the data by the next CH in C_{n-1}. Data is encrypted using cluster secret key $S_{n-1}$by performing XOR as in step 1
Step 5: The encryption process using XOR continues through inter-cluster communication until it reaches to BS.
Step 6: Data is transmitted through inter-cluster communication until it reaches to BS. BS can decrypt the data by performing XOR of data with all secret keys S_i which is given by

$$D_i = S_1 \oplus S_2 \oplus S_3 \dots . \oplus E_n$$

Trust degree computation

In this section dynamic trust degree values of sensor nodes are calculated. The trust values are dynamically evaluated for each sensor node, initially sensor nodes are trustworthy and assigned with trust value of 0.5 and it is periodically monitored based on its activities. The CH authenticates its sensor by secret key given by BS and collects data from sensor (CM). The trust value between two sensors is given as

$$if\ A_{CH} \geq B_n$$

$$T_{transmission} = 1 - \frac{1}{\left\{\frac{A_{CH}-B_n}{A_{CH}+B_n} * W_s\right\}+2} \quad (1)$$

$$if\ A_{CH} < B_n$$

$$T_{transmission} = \frac{1}{\left\{\frac{B_n-A_{CH}}{A_{CH}+B_n} * W_u\right\}+2} \quad (2)$$

Based on number of successful and unsuccessful transmission between cluster head and sensor node is represented as A_{CH} and B_n and their weights are given as W_s and W_u respectively. For successful transmission $T_{transmission}$ the trust value ranges from $(0.5 - 1)$ and for unsuccessful transmission $T_{transmission}$ is less than (0.5)

The trust value of sensor nodeB_n is computed by CH A_{CH} based on its recommendation is given as

$$T_{trust} = \frac{\sum_{i \neq A_{CH}, i \neq B_n} T_{A_{CH}}^{i} * T_i^{B_n}}{\sum_{i \neq A_{CH}, i \neq B_n} T_{A_{CH}}^{i}} \quad (3)$$

$T_{A_{CH}}^{i}$ is trust of CH and $T_i^{B_n}$ is trust value of sensor transmitted by node to CH.

Trust value computed by CH for its sensor in the current time is given as

$$T_{trust} = W_e T_{transmission} + W_r T_{trust} \quad (4)$$

where $W_e + W_r = 1$

$W_e and W_r$ represents weights of trust experience and recommendation respectively.

V. SIMULATION EXPERIMENTS AND RESULTS

In this section the performance analysis of proposed TBSK is carried on discrete event simulation tool NS2. The simulation experiment is carried out and scenarios are analysed. The proposed TBSK is compared with the existing trust based routing TSRF [24] and LWTM [25]. The robust of the proposed TBSK scheme against malicious behaviour is analysed. Initially all the sensor nodes are considered non-malicious (trustworthy) considering non-malicious nodes successfully interact with other node and reports positive feedback, while malicious node (untrustworthy) does unsuccessful interaction, reports false and negative feedback. In our scenario we consider blackhole and greyhole attack which has greater impact to reduce overall network performance. In our experiment we deploy 200 nodes and clustering formation is done [22] accordingly. Malicious nodes are varied from 1 to 10 in network. In greyhole attack the malicious node tries to drop few packets and refuse to forward to destination. In our TBSK scheme the CM forwards trust degree value to CH. CH evaluates its CM trust values and forwards it to BS. Whenever malicious node advertises itself having better route, the neighbour recommendation and trust value increases. However $T_{transmission}$ for malicious node will be low, due to packet drop and trust value of malicious T_{trust} will be above 0.5. To detect such kind of malicious activity CH evaluates trust degree and matches with the trust value given by CM and secures the intra-cluster communication before sending to BS. In blackhole attack, node intentionally drops all the packets and make easy to detect compared to greyhole. CH does not select node for routing if trust degree is less than threshold value. Simulation parameters used is shown in Table 1.

Table 1: Default simulation parameters

Simulation Parameters	Value
Network area	1000x1000
Clustering	Fuzzy-LEACH
No of nodes	200
Mac layer	802.11
Transmission range	250mts
Traffic	CBR
Simulation time	100 sec
Initial energy	50J
Packet size	512bytes
Simulation Rounds	5,10,15
Malicious nodes	1to10
Data Rate	2mb

PERFORMANCE METRICS

A. THROUGHPUT

It is number of packets received at destination per unit time, efficiency of the network is reflected by throughput. Throughput is given as:

$$Throughput = \frac{m_1}{m_2} \times 100\ \%$$

where m_1 and m_2 is the packet received by destination and packet sent by source. Throughput is measured in kbps. Figure 2 shows the throughput graph of TBSK with comparison of TSRF and LWTM under malicious nodes. By exploring experimental scenarios, it is observed that throughput of TBSK is more compare to other scheme. Since TBSK has robust in selecting reliable routes to BS by incorporating security measures. Other scheme lacks to detect network conditions in presence of malicious nodes which lead to decrease overall throughput.

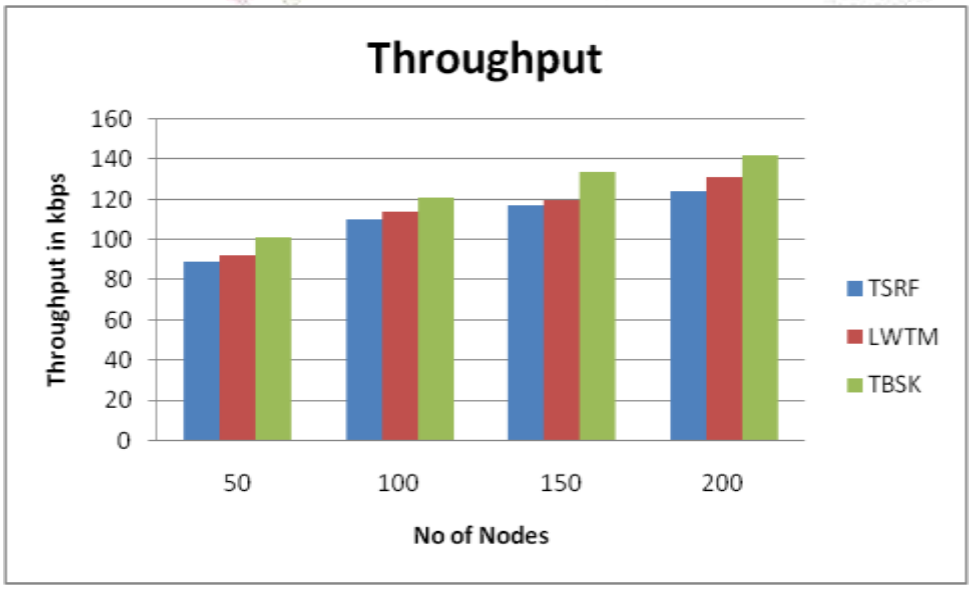

Figure 2: Throughput vs Network size graph

B. PACKET DELIVERY RATIO (PDR)

It is ratio of total number of packet generated at source to the ratio of total number of packet received at destination. PDR is given as:

$$PDR = \frac{Total\ number\ of\ packet\ received}{Total\ number\ of\ packet\ sent} \times 100$$

It is observed that in proposed TBSK scheme the packets are delivered efficiently by computing trust degree of each node. Only trusted nodes are selected for routing data packets thus increasing the packet delivery ratio. Figure 3 shows the PDR graph, we can observe that TBSK scheme delivers more successful transmission compared to TSRF and LWTM, the malicious nodes are varied and checked for successful transmission rate and packet loss in presence of malicious nodes. Our scheme outperforms better than TSRF and LWTM achieving high packet deliver ratio with lesser packet loss. Figure 4 shows the false positive number in presence of malicious node. It is seen that the false positive number increases in TSRF and LWTM, as nodes reports false recommendation and nodes get compromised to attacker. But TBSK recommends based on the trust value and reports positive.

C. END-TO-END DELAY

It is mean value delay between sent time and arrival time of nodes. It is total amount of time taken by source node for transmitting packet to destination. Delay can be given as:

$$Delay = \sum \frac{(T_1 - T_2)}{N}$$

where $T_1\ and\ T_2$ are time of first packet arrival at destination and time of first packet sent from source. Number of packets is represented as N. Figure 5 shows the delay graph since TBSK selects trusted node while routing data packets.

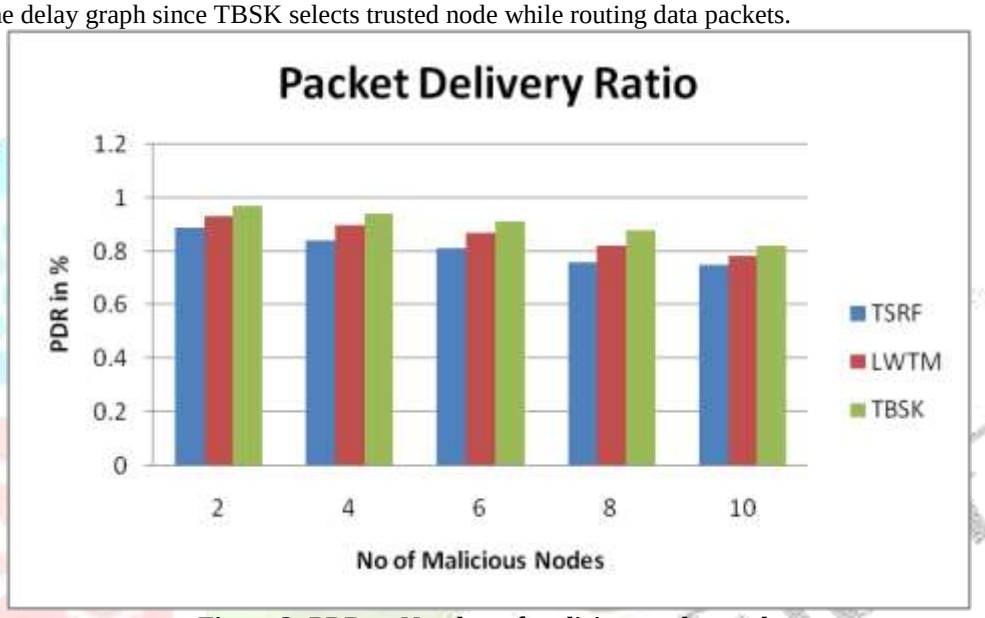

Figure 3: PDR vs Number of malicious node graph

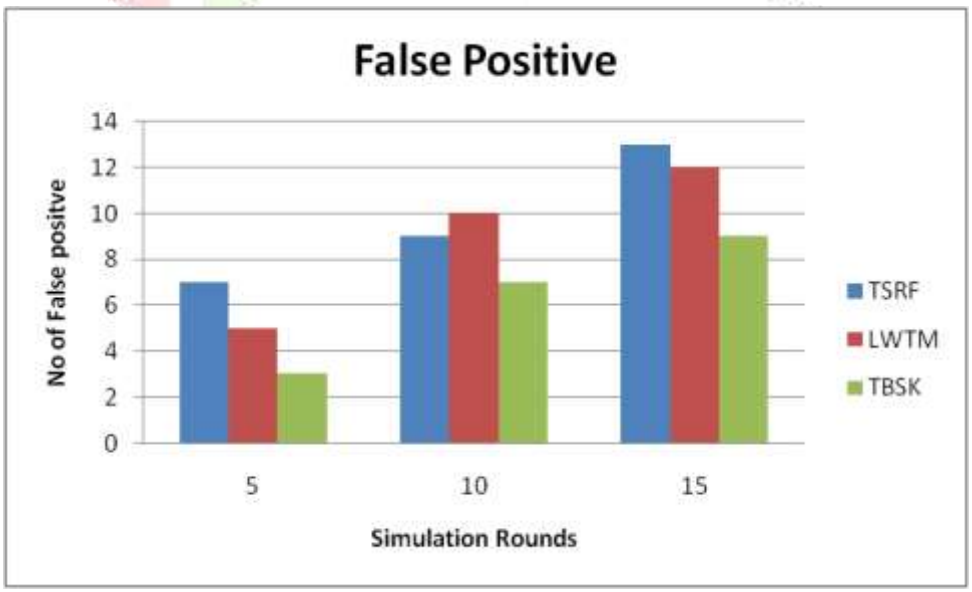

Figure 4: False positive vs simulation round graph

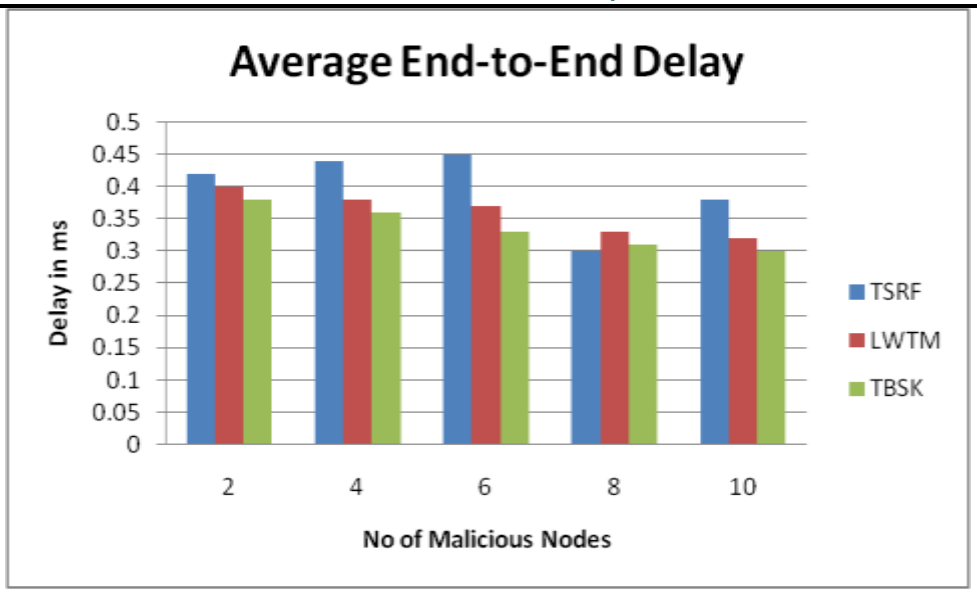

Figure 5: Average delay vs Number of Malicious node graph

The delay in establishing route to BS is low compared to TSRF and LWTM. Due to packet drop of misbehaviour of nodes, the retransmission through alternate routes increases delay. It is observed that TBSK scheme selects trusted nodes for successful transmission thus decreases delay.

D. ROUTING OVERHEAD

Routing overhead gives vital influence on evaluating routes to destination to forward data. Routing overhead is given as:

$$Routing\ Overhead = \frac{N_1}{N_2}$$

where N_1 are number of routing packets sent and forwarded, N_2 is number of data packets received. Increase in the number of malicious nodes causes more overhead in computing route and retransmissions to destination. The TBSK has low overhead compared to TSRF and LWTM, as reliable trusted paths are constructed based on trust degree and the lightweight secret key shared by BS. However cryptographic functions are reduced compared to LWTM which results high routing overhead. Figure 6 shows routing overhead graph.

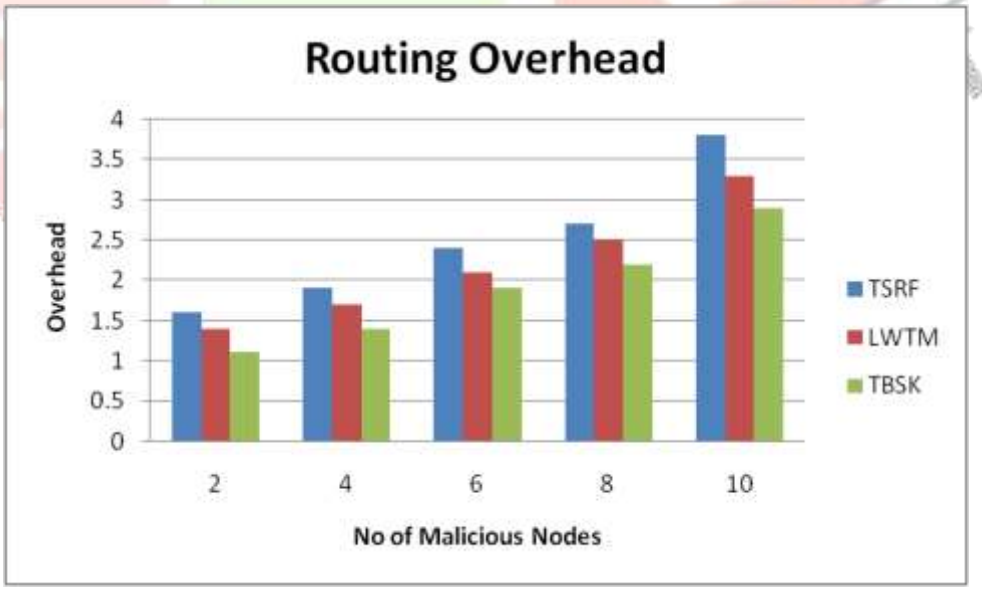

Figure 6: Routing overhead vs Number of Malicious nodes

VI. CONCLUSION

It is necessary to provide security for nodes to mitigate attacks and achieve QoS for secure and reliable data transmission. This paper presents Trust Based Secure Key sharing scheme (TBSK) for hierarchal cluster which aims to detect malicious activities in the network by using lightweight XOR key sharing to reduce the overhead of the nodes. Secret keys are shared by BS to corresponding clusters, malicious activities of sensor node are detected by computing dynamic trust degree of individual sensor node by CH for successful and unsuccessful transmission. BS verifies inter-cluster by XOR-ing corresponding cluster secret keys. Simulation experiments shows the proposed TBSK scheme outperforms existing trust based routing scheme TSRF and LWTM in terms of throughput, packet delivery ratio, average end-to-end delay and overhead. In future to reduce cryptographic computation lightweight dynamic threshold key management scheme can be used to detect malicious activities by changing the keys at different threshold time.

REFERENCES

[1] T. Park and K. G. Shin. 2004.LiSP: A Lightweight Security Protocol for Wireless Sensor Networks, ACM Trans. Embedded Comput. Syst., 3(3): 634-660.

[2] E. Shi and A. Perrig. 2004. Designing Secure Sensor Networks, IEEE Wireless Commun., 11(6): 38-43.

[3] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song. 2006. Trust Management Problem in Distributed Wireless Sensor Networks, in Proc. 12th IEEE Int. Conf. Embedded Real-Time Comput. Syst. Appl. (RTCSA), 411-414.

[4] M. A. Mahmood, W. K. G. Seah, and I. Welch. 2015. Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead, Comput. Netw. 79: 166-187.

[5] K.-A. Shim. 2016. A Survey of Public-key Cryptographic Primitives in Wireless Sensor Networks, IEEE Commun. Surveys Tuts., 18(1): 577-601.

[6] Y. Yu, K. Li, W. Zhou, and P. Li. 2012. Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures, J. Netw. Comput. Appl., 35(3): 867-880.

[7] I. Butun, S. D. Morgera, and R. Sankar. 2014. A Survey of Intrusion Detection Systems in Wireless Sensor Networks, IEEE Commun. Surveys Tuts., 16(1): 266-282.

[8] F. Ishmanov, S. Kim, and S. Nam. 2014. A Secure Trust Establishment Scheme for Wireless Sensor Networks, Sensors, 14(1): 1877-1897.

[9] F. Ishmanov, S. Kim, and S. Nam. 2015. A Robust Trust Establishment Scheme for Wireless Sensor Networks, Sensors, 15(3): 7040-7061.

[10] S. Talbi, M. Koudil, A. Bouabdallah, and K. Benatchba. 2017. Adaptive and Dual Data-communication Trust Scheme for Clustered Wireless Sensor Networks, Telecommun. Syst., 65(4): 605-619.

[11] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho. 2012. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-based Routing and Intrusion Detection, IEEE Trans. Netw. Service Manage., 9(2): 169-183.

[12] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song. 2009. Group-based Trust Management Scheme for Clustered Wireless Sensor Networks, IEEE Trans. Parallel Distrib. Syst., 20(11): 1698-1712.

[13] A. Boukercha, L. Xu, and K. El-Khatib. 2007. Trust-based Security for Wireless Ad Hoc and Sensor Networks, Comput. Commun., 30(11-12): 2413-2427.

[14] J. Zhang, R. Shankaran, A. O. Mehmet, V. Varadharajan, and A. Sattar. 2010. A Trust Management Architecture for Hierarchical Wireless Sensor Networks, in Proc. IEEE Local Comput. Netw. Conf., 264-267.

[15] X. Li, F. Zhou, and J. Du. 2013. LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks, IEEE Trans. Inf. Forensics Security, 8(6): 924-935.

[16] N. Karthik and V. S. Ananthanarayana. 2017. A Hybrid Trust Management Scheme for Wireless Sensor Networks, Wireless Pers. Commun., 97(4): 5137-5170.

[17] W. Fang, C. Zhu,W. Chen,W. Zhang, and J. J. P. C. Rodrigues. 2018. BDTMS: Binomial distribution-based Trust Management Scheme for Healthcareoriented Wireless Sensor Network, in Proc. 4th Int. Wireless Commun. Mobile Comput. Conf., 382-387.

[18] J. Górski and A. Turower. 2018. A Method of Trust Management in Wireless Sensor Networks, Int. J. Secur., Privacy Trust Manage., 7(3): 1-19.

[19] A. K. Gautam and R. Kumar. 2018. A Robust Trust Model for Wireless Sensor Networks, in Proc. 5th IEEE Uttar Pradesh Section Int. Conf. Electr., Electron. Comput. Eng. (UPCON), 1-5.

[20] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo. 2019. LB-IDS: Securing Wireless Sensor Network using Protocol Layer Trust-based Intrusion Detection System, J. Comput. Netw. Commun., Art. no. 2054298.

[21] S. Din, A. Paul, A. Ahmad, and J. H. Kim. 2019. Energy Efficient Topology Management Scheme Based on Clustering Technique for Software Defined Wireless Sensor Network, Peer-to-Peer Netw. Appl., 12(2): 348-356.

[22] P. Nayak and A. Devulapalli. 2016. A Fuzzy Logic-based Clustering Algorithm for WSN to Extend the Network Lifetime, IEEE Sensors J., 16(1): 137-144.

[23] W. Abidi and T. Ezzedine. 2017. Fuzzy Cluster Head Election Algorithm Based on LEACH Protocol for Wireless Sensor Networks, in Proc. 13th Int.Wireless Commun. Mobile Comput. Conf. (IWCMC), 993-997.

[24] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao. 2014. TSRF: A Trust-aware Secure Routing Framework in Wireless Sensor Networks, Int. J. Distrib. Sensor Netw., 10(1): Art. no. 209436.

[25] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar. 2017. A Lightweight Trust Mechanism and Overhead Analysis for Clustered WSN, IETE J. Res., 63(3): 297-308.

AUTHORS PROFILE:

[1]**Dr. Lata B T** is an Assistant Professor in the Department of Computer Science and Engineering at University Visvesvaraya College of Engineering. Bangalore University, Bengaluru, India. She obtained her B.E in Computer Science and Engineering from Karnataka University, Dharwad and M.Tech degree in Computer Network Engineering from Visvesvaraya Technological University, Belgaum. Ph.D degree in the area of Wireless Sensor Networks from Bangalore University. Her research interest is in the area of Sensor Networks, IOT and Image processing.

[2]Dr. Venugopal K R, is currently the Vice Chancellor, Bangalore University, Bengaluru. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D in Economics from Bangalore University and Ph.D in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE and ACM Distinguished Educator.