DOI: http://dx.doi.org/10.26483/ijarcs.v12i5.6769

Volume 12, No. 5, September-October 2021

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A REVIEW OF DIFFERENT TECHNIQUES WHILE TRUST NODE ESTIMATION IN A HIERARCHICAL WIRELESS SENSOR NETWORKS

Rahul Das, Dr. Mona Dwivedi
Mansarovar Global University,Billkisganj,Sehore
,Madhya Pradesh,India

Abstract: When we considered a wireless sensors network, the safety measures have been create depending on non-realistic trusted environment. Some malicious sensor nodes may illegally drop the data packets and disturb network communication. Hence, internal networks attacks of malicious nodes becoming a challenging research topic under on its trust and security solutions for WSN. After analysing the trust mechanism schemes for wireless sensor networks, it has been found that there are different trust mechanism schemes are present. Every scheme has several advantages for finding a better path for source to destination node. In this paper, a review on different trust estimation schemes in WSNs is carried out which are classified.

Keywords*:* Trust estimation, Cluster head, security, wireless sensor network, sensor node, wsn,BS.

1. INTRODUCTION

For un-unique features of WSNtrust management and evaluation has several issues. The complexity of monitoring the node behaviour, evaluation and management of trust increase non-linearly as the nodes increases. Therefore, itis a greater challenge to neighbor nodes to performing the trust estimation and management by node .To overcome the security issues, trust assessment is necessary to be act as a protect mechanism to collects data from the intermediate node by monitoring the sensor network to be send to the base station (BS).To identify the malicious node Trust management is one of the way which be authenticated. Trustapproachbecomes more challenge and significant as the reality of sensor nodes has special character and limited resources.Therefore, a suitable and efficient mechanism is necessary to identify the malicious node and minimize the loss in network by selecting proper CH [Fig1]. The trustworthy communication between the clustered nodes belong to the integrity and reliability of collected information.Thus,improving security and robustness the present research focus on trust on nodes in HWSN of presenting trust evaluation. Applying already exist security solutions such as hash function, authentication, and cryptography only present security up to certain extent. But malicious nodes finding of has large complexity in computation and energy consumption. There is a technique trust-based mechanism that is introduced which is betterin term of reliability and efficient of detecting the malicious nodes than traditional cryptographic techniques .

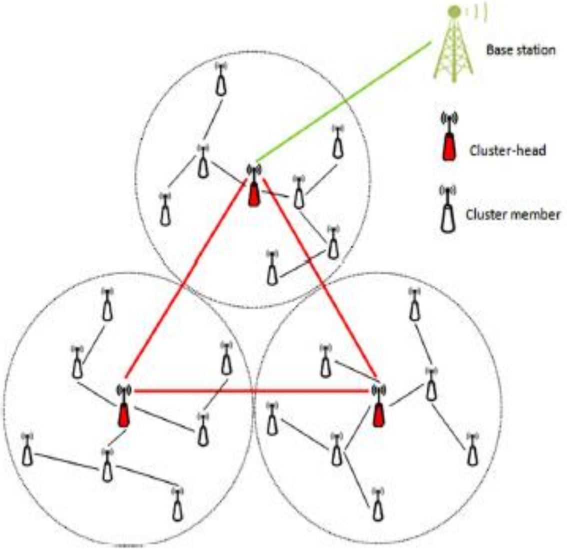

Figure 1: Formation of cluster-based HWSN

2. TRUST IN SENSOR NETWORKS

Constructing the network and making the addition and/or deletion of sensor nodes from a networkTrust in WSN networks plays an important role , due to the growth of the network, or the replacement of failing and unreliable nodes very smooth and transparent.The trust establishment between nodes is a mustas the creation, operation, management and survival of a WSN are dependent upon the cooperative and trusting nature of its nodes. However, using the traditional tools such as cryptographic tools to generate trust evidence and establish trust and traditional protocols to exchange and distribute keys is not possible in a WSN, due to the resource limitations of sensor nodes [11]. Therefore,to secure communication and distribution new innovative methods of trust values between nodes are needed. Trust in

WSNs, has been studied lightly by current researchers and is still an open and challenging field.

3. RELATED WORK

[3.1]-MFCTE

MFCTE[1] Means Multi-Level Fuzzy Cluster Based TrustEstimation for Hierarchical Wireless SensorNetworks. The trust is computed based on communication trust, energy trust, and data trust. The total trust estimation is performed in CH and BS. The operation on the CH and BS is performed using a fuzzy decision making process to detect good, bad and uncertain nodes. In the intra-cluster level, the direct trust is estimated by Cluster Member (CM) to CM within the cluster and CH estimates the trust of CM of its cluster for indirect trust calculation. In inter-cluster level, the direct trust is estimated between CH -CH and the indirect trust evaluation is performed by the BS based on the trust information calculated by the CH.Thus, Multi-level fuzzy model is used of its easy nature and of capturing the expert knowledge. The four level of operation performed are Fuzzification, Fuzzy rules creation, Fuzzy interference system, and Defuzzification.

[3.2]-ADCT

ADCT[2] means an adaptive and dual data communication trust protocol.ADCT that operates on two levels namely, intra-cluster and inter-cluster levels. Distributed and centralized approaches are used by these two levels for trust evaluation. each cluster member (respectively cluster-head) processed individual trust values in distributed approach for its neighboring nodes in the cluster (respectively in WSN) to make decision about their trustworthiness according to a defined trust threshold. a cluster-head (respectively base station) build a feedback for each member (respectively each cluster head) in the centralized approach, based on the recommendation values (i.e., previouslycomputed on the distributed approach) received from other members (respectively from other cluster-heads).

[3.3]-SNTEM

SNTEM[3]means a Software-based node-level trust evaluation method that aims the trust at node level by using the available internal resources without non-cryptographic technique and lesser energy overheads in the network. This model consists of two stages which include the challenge-response (CR) model and node-level trust evaluation task. In the first stage, the destination node is trusted by performing a comparison between the response and the challenge estimated at the source node. The second stage is categorized under three levels where node Conditioning is performed based on the lookup table and Immutable Response. Next, the Self-scrutiny algorithm deployed node by Sequential boot check method. Finally, a Self-attestation algorithm enables the communication among source and destination within its range in peer-peer mode. However, two nodes with the same node memory are trusted otherwise it was not trustworthy.

[3.4]-BLTM

BLTM[4] means Beta and Link Quality Indicator based Trust Model (BLTM) that calculate the trust relationship between the sensor nodes. This model consists of five modules such as Link Quality Indicator (LQI) analysis, direct trust, recommendation trust, integrated trust, and trust update-modules. Firstly, the source node collects LQI data within the destination node and its link quality is good to continue the trust calculation. The three metrics such as energy, communication, and data trust which are used to calculate direct trust value and combine the value of two nodes. Next, the integrated trust was calculated by the weight of direct trust and recommendation trust. Finally, the trust values are updated by using a sliding time window. Although it reduces poor quality links this method could not defend DOS and Data tampering attacks.

[3.5]-BTEM

BTEM[5]means Belief based Trust Evaluation Mechanism (BTEM) detach the malicious node and protect against On-off and Bad-mouthing attacks. This mechanism has three modules such as the Traffic Monitoring module, Trust Evaluation module, and Decision Maker. At first, the source node with a transmission range forward data to the destination node, and it was monitored by a traffic profile to identify the malicious node. The three metrics are traffic receiver, direct trust, and indirect trust evaluate trust nodes in communication range receive packet tuned on the same channel by Bayesian Estimation approach. Finally, the Decision Maker module compares the threshold value ranges with the probability of each node. However, to identify the malicious nodes are a challenging task due to computation complexity, large memory requirements, and high energy consumption.

[3.6]-ETRES

ETRES[6]means an Exponential based Trust and Reputation Evaluation System (ETRES) which estimates the distributed trust node. This model consists of three models consists of Trust and Reputation modeling, Trust and Reputation Estimation Modelling, and Exponential based trust modeling. According to the relationship between beta distribution and exponential distribution, the nodes calculate their trust value based on the time interval between the adjacent nodes. Then the entropy-based confidence factor saves the computing node power to consume low energy. Finally, trust value calculated by an interaction between the nodes. However, selective forwarding, on-off, slander, and collusion attack reduce the lifetime of the network.

[3.7]-LTS

LTS[7]means Light Weight Estimation Trust Scheme (LTS) to improve the trust of clustering and security to defend a malicious attack. This model operated in two phases such as intra-cluster trust level, inter-cluster trust level along with centralized and distributed approaches where the unique identifier is given to each sensor node to communicate with the destination node. First, the trust level occurs at minimum communication overhead with high capability detection and monitor the sensor node by its intermediate node. Next, consider the communication trust and evaluate the indirect trust by a base station and examine scalability and convergence rate of LTS to optimize the cluster. However, the storage memory is low due to on-off and collusion attacks.

[3.8]-HTMS

HTMS[8]means a Hybrid Trust Mechanism Scheme (HTMS) to detect data fault used by spatial and temporal relationships and recover the untrusted data. This model depends upon three phases such as data trust evaluation, node trust evaluation, and trust score adjustment. Initially, data item sent to the sink node through its intermediate node and then allot the data trust score calculated by self-data trust, peer- data trust. Then, node trust value was evaluated by the sliding window. Finally, trust score adjustment based on provenance based trust done by a sink node to detect data fault. This approach destroys the information of sensor nodes due to on-off, bad-mouthing attacks.

[3.9]-TSSRM

TSSRM[9] means aTrust Sensing based Secure Routing Mechanism (TSSRM) to handle network attacks. This model consists of three phases such as Network initialization process, route construction process, and route maintenance method. At first, the cluster head was selected by monitoring the node with its neighbor node and exchange its trust degree. Next, construct the transmission link which controls the transmission range and direct trust, indirect trust, and incentive factor detect the nodes with the attack. Finally, new nodes are joined due to route update and handle the route repair initiated by node movement. This approach was difficult to ensure the multi-hop information transmission security.

[3.10]-MTIDS

MTIDS[10]means Multi-agent trust-based Intrusion Detection Scheme (MTIDS) to detect the node intrusion and trusted value of the node.ByMahalanobis distance theory First, the attributes of the node to assigned and check whether attributes are normal. According to the combination of beta distribution and a tolerance factor the sensor, the node transmits data to cluster head calculate and update the reputation distribution of node trust. The tolerance factor detects the false rate of the node. Finally, compare the trust value with the threshold value to detect node intrusion. However, the multiple types of intrusion occur then decrease the detection rate of the node.

Table 1 has clearly shown comparison among available techniques. However comparisons have clearly shown that the combination of all techniques compared with reviewed paper to find which technique is perform better than the available methods to improve the energy enhancement & lifetime of network in wireless sensor networks.

Table -1: Various techniques described through following comparison.

Year	Technique	Features	Advantages	Drawback
2020	MFCTE	The trust is computed basedoncommunication trust, energy trust, and data trust.	Low energy,Save computing power,Increase network lifetime,Detect malicious nodes	Distance enforcement between CHs is proposed which defects against malicious nodes.
2019	SNTEM	Enable the communication amongsource and destination within its range in peer-peer mode	Low energy overheads in the network	Difficult to generate trusted node due to its different memory size
2019	ETRES	Trust value calculated by interaction between the nodes.	Save computing power, low energy consumption	Prone to Selective forwarding, on-off, slander and collusion attack which increases the lifetime of the network.
2019	BLTM	evaluate the trust relationship between the sensor nodes, trust values are updated by using sliding time window	LQI data detect external node intrusion	Does not defend DOS and Data tempering attacks.
2019	BTEM	Isolate the malicious node and protect against On-off and Bad-mouthing attacks	Increase network lifetime	High computation complexity, large memory

				requirements
2019	LTS	high capability detection, monitor the sensor node by its intermediate node	Improve security and reliability of the node	Problem in storage memory due to on-off and collision attacks
2017	HTMS	Detect data fault used by temporal and spatial correlation.	Recover untrusted data, provide attack residence degree	Destroy the information of sensor nodes due to on-off, bad-mouthing attacks.
2017	MTIDS	Detect node intrusion and trusted value of node	Detect malicious nodes	Decrease detection rate of node due to multiple types of intrusion occurs
2017	TSSRM	Cluster head monitor the node with its neighbor node, control the transmission range	Efficient and reliable data transmission	Reduce routing overhead.
2016	ADCT	operates on twolevels namely, intra-cluster and inter-clusterlevels. Two levels usesa distributed and centralized approaches for trust evaluation.	DealwithuntrustworthyrecommendationsMulti-attribute basedcommunication trust	High computing power, High energy consumption

4. CONCLUSION

From disparate scientific fieldstrust as an essential and important attribute in building a relationship between entities has been studied for a long time by scientists.It is very crucial issue toTrustevalution due to the nature of wireless sensor nodes. In this paper first we have discussed the trust in WSN, then explain various models for trust node estimation in WSN.The sensing technology has made it possible for any sensor node to communicate and respond to the different attributes.This paper has briefed about various aspects in WSN. Every field has examined modelling and calculating trust using different techniques, and one of the most prominent and promising techniques is the use of statistics, mainly probabilities to solve the problem, especially in dynamic networks where the topology is changing rapidly. system andthe existing methods to detect the malicious node inwireless sensor network.

5. REFERENCE

1) Das R,DwivediM,.Multi-Level Fuzzy Cluster Based TrustEstimation for Hierarchical Wireless SensorNetworks. International Journal of Next-Generation Computing, Vol. 11, No. 3, November 2020. (pp. 263-280).
2) Talbi S, Koudil M, Bouabdallah A, Benatchba K. Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. Telecommunication Systems. 2017 Aug 1;65(4):605-19.
3) Desai SS, Nene MJ. Node-level trust evaluation in wireless sensor networks. IEEE Transactions on Information Forensics and Security. 2019 Jan 21;14 (8):2139-52.
4) Wu X, Huang J, Ling J, Shu L. BLTM: Beta and LQI Based Trust Model for Wireless Sensor Networks. IEEE Access. 2019 Mar 18;7: 43679-90.
5) Anwar RW, Zainal A, Outay F, Yasar A, Iqbal S. BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks. Future Generation Computer Systems. 2019 Jul 1;96:605-16.
6) Zhao J, Huang J, Xiong N. An effective exponential-based trust and reputation evaluation system in wireless sensor networks. IEEE Access. 2019 Mar 12;7:33859-69.
7) Khan T, Singh K, Abdel-Basset M, Long HV, Singh SP, Manjul M. A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks. IEEE Access. 2019 May 3;7:58221-40.
8) Karthik N, Ananthanarayana VS. A hybrid trust management scheme for wireless sensor networks. Wireless Personal Communications. 2017 Dec 1;97(4):5137-70.
9) Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q. Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access. 2017 May 23;5:9599-609.
10) Jin X, Liang J, Tong W, Lu L, Li Z. Multi-agent trust-based intrusion detection scheme for wireless sensor

networks. Computers & Electrical Engineering. 2017 Apr 1;59:262-73.

11) L. Eschenauer, "On Trust Establishment in Mobile Ad-hoc Networks", in Department of Electrical and Computer Engineering, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.