Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Multi Trust-based Secure Trust Model for WSNs

Tayyab Khan*

*Corresponding author, School of Computer and Systems Sciences, JNU, New Delhi- 110067, India. E-mail: tayyabkhan.cse2012@gmail.com

Karan Singh

Ph.D., SCSS, Jawaharlal Nehru University, New Delhi, India. E-mail: karan@mail.jnu.ac.in

Sakshi Gupta

School of Computer and Systems Sciences, JNU, New Delhi- 110067, India. E-mail: guptasak1396@gmail.com

Manisha Manjul

Department of Computer Science and Engineering, G B PEC, New India. E-mail: manishamanjul@gbpec.edu.in

Abstract

Trust establishment (TE) among sensor nodes has become a vital requirement to improve security, reliability, and successful cooperation. Existing trust management approaches for large scale WSN are failed due to their low cooperation (i.e., dependability), higher communication and memory overheads (i.e., resource inefficient). This paper provides a new and comprehensive hybrid trust estimation approach for large scale WSN employing clustering to improve cooperation, trustworthiness, and security by detecting selfish sensor nodes with reduced resource (memory, power) consumption. The proposed scheme consists of unique features like authentication based data trust, scheduler based node trust, and attack resistant by giving the high penalty and minimum reward during node misbehavior. A task scheduling mechanism is employed for scheduling the significant task to reduce computation overhead. The proposed trust model would be capable to provide security against blackhole attack, grey hole attack, and badmouthing attack. Moreover, the proposed trust model feasibility has been tested with MATLAB. Simulation results exhibit the great performance of our proposed approach in terms of trust evaluation cost, prevention, and detection of malicious nodes with the help of analyzing consistency in trust values and communication overhead.

Keywords: Trust management, Resource scheduling, Attacks, WSN.

DOI: https://doi.org/10.22059/jitm.2022.86657 Manuscript Type: Research Paper University of Tehran, Faculty of Management

Received: January 12, 2021 Accepted: March 25, 2021

Introduction

Wireless sensor networks (WSNs) are collections of several small sizes self-organized low-cost resource constraint (memory, power, processor, bandwidth and short communication range) sensor nodes (SNs) which mainly deployed in the hazardous (hostile) area. Sensor nodes (SNs) monitor events, collect continuous and discrete data, and sent (report) to the base station (sink node). WSNs nodes communicate via radio links with limited available bandwidth and form a temporary network, i.e., network without predefined infrastructure and centralized network administration (Boukerche et al., 2007) (Basan et al., 2016) (He et al., 2012). WSN uses a highly dynamic network topology where, any time, sensor nodes can leave and join a network and change their locations. Due to the deployment (distributed, dynamic and collaborative) nature of WSNs, sensor nodes are less reliable, failure-prone and prone to several attacks like blackhole attack, on-off attack, Sybil attack, etc. (Crosby et al., 2006) (Ganeriwal et al., 2008) (Jiang et al., 2015). Once a node is compromised by adversary force having access to cryptographic keys to access other nodes of WSNs, erroneous data routing by malicious (faulty, selfish, bad or spiteful) nodes will breakdown the entire network. In such cases, when the WSNs node itself becomes a malicious node and due to resource constraints or limitation of WSNs nodes, cryptographic techniques cannot prevent from internal attacks (Ishmanov et al., 2015). Thus we need a different kind of robust security mechanism to prevent WSNs from internal and external attacks known as Trust Estimations mechanisms in wireless sensor networks. Trust estimation (TE) methods are used to evaluate the dependability and reliability of sensor nodes for the survival of wireless sensor nodes (Jadidoleslamy et al., 2016). LEACH, EEHC, and EC provide good clustering scheme to enhance the network measurability and throughput. Within a cluster, a cluster with a sufficient number of resources (CPU, power, memory) is selected as a cluster head that monitors the cluster member nodes and states the degree of trustworthiness. Cluster head identifies the malicious nodes within the cluster and selects the reliable route to transmit the data. The altered information about the trustworthy (genuine) SNs of the whole network is maintained in a database. Size of Database and size of the network are directly proportionally to each other. It is unfeasible for a single node (Bin Ma et al., 2009) to store, compute, and monitor the trust values with alteration of the whole network. To reduce the communication and memory overheads, we have scheduled the task using a well-known algorithm (Riaz et al., 2009) and eliminate the unnecessary feedbacks from selfish nodes. In this paper, a specialized dataset for WSN is used (Tan et al., 2015) to detect and mitigate various internal attacks like bad mouthing attack, blackhole, and grey hole attacks. Rest of the work is divided into following sub-sections. Table 1 indicates a comparative analysis of these trust models in terms of various parameters. There are various methods and approaches to model trust, like probability, fuzzy, weighted, Bayesian, game theory, entropy-based, neural network . Usually, Trust Establishment schemes have been considered as a useful and effective tool to enhance security and dependability (cooperation).

Table 1. Comparative analysis of the various existing state of the art trust models.

Trust model	Architecture	Key objectives (Purpose)	Basis of computation	Observation	Limitation	Complexity
TCHEM (Crosby et al., 2006)	Hierarchical (or distributed)	Selection of trusted Cluster head (CH)	Node behavior, TDM	Importance of trustworthy cluster head selection in cluster-based trust models	Not comprehensive, no sharing of the trust value	High
ATRM (Boukerche et al., 2007)	Hierarchical	Overhead reduction	Agent, certificate-based	MN to SN and vice versa	Unrealistic (due to the assumption made)	Minimal
HTCW (Zhou et al., (2009)	Hybrid	Trust-based network security to detect malicious behavior of nodes	Beta distribution, surveillance nodes, and watchdog mechanism	Reduction in CH resources and future behavior prediction of nodes	Suitable for limited size clusters and CH can be easily compromised. Only Sybil and replication attack resilient	High delay with excess message overheads introduced by surveillance node
NBBTE (Feng Zhou	Distributed	Node behavior based Trust estimation	Weight (fuzzy theory and D-S	Analyzed the influence of malicious behavior	Communication and memory overhead varies	Higher (due to its excess

et al., 2011)			evidence theory)		with network density. Only on-off attack resilient	energy and memory requirement)
TMBBT (Liu et al., 2011)	Hybrid	Building an adaptive and energy efficient trust model to resolve the multi-hop neighborhood trust issue	Bayes theorem	Data trust, communication trust, and history collectively used to obtain reputation. Suitable for multihop routing	Data and communication trust aggregation method is not defined. Only bad mouthing and conflicting behavior attack resilient	Minimal
GTMS (Shaikh et al., 2008)	Hybrid	Communication and memory overhead reduction	Group	Trust calculation at the node, CH and BS level	Low dependability and malicious attacks such as on-off, conflicting behavior attack, etc. are not considered against the trust model. moreover punishment coefficient is static and weak	High (due to broadcast strategy)
HTMP (Bao et al., 2012)	Hierarchical	Security improvement	Geographic	Station to CH, CH to CM Peer to peer	Unrealistic (Malicious feedbacks are not considered in trust evaluation), and implementation is relatively difficult.	Higher (due to complex trust estimation scheme)
LDTS (Li et al., 2013)	Hybrid	Overheads reduction and security improvement	Weight	Intercluster: BS to CH, CH to CH Intracluster: CH to CM, CM to CM	static punishment coefficient used by trust function cause security issues	minimal (Calculation and communication overhead)
ML-TRUST Zhang et al., 2014)	Distributed	Multilevel and subjective-objective based TMS	Weight	Only communication trust is considered for trust estimation	Sharing and renewal of trust are not considered. moreover, data trust is not considered for trust estimation	High
(Ishmanov et al., 2015)	Distributed	Lightweight and robust TMS	Weight	Misbehavior component is used to monitor the persistency of malicious nodes. Forgetting factor is also introduced	bit sensitive to false positive alarms. suitable for static WSN	Minimal
EDTM (Jiang et al., 2014)	Distributed	Develop an Efficient trust model	Weight	Data, communication, and energy trust are considered for trust estimation	Selection of suitable weight and threshold	High (calculation overhead)
DBTA (Won et al., 2015)	Centralized	Distance-based TMS	Weight	Only data trust along with correlation is considered for trust estimation	Communication trust is not considered . not robust against on-off attack	High
ADCT (Talbi et al., 2017)	Hybrid	Data communication TMS based on adaptive trust function and past interaction	Non-linear	Only data and communication trust are considered for trust estimation	Only spatial correlation is used for data trust	Minimal
DTMS (Jadidoleslamy et al., 2016)	Distributed	Data similarity and available resource based fuzzy TMS	Fuzzy	Available resource, data, and communication trust are considered for trust estimation	Not robust against spoofing and Sybil attack	Minimal
MultiProTru (Dogan et al., 2017)	Distributed	Kalman filtering and provenance-based trust	Kalman filtering	Filtering untrusted data. Only data trust is considered for TMS	Attack resiliency and communication trust is not considered. suitable for a static environment	High
LWTM (Singh et al., 2017)	Hybrid	Design a realistic TMS with reduced overheads	Weight	Intra-cluster: CM to CM ,CH to CM Inter-cluster: CH to CH, BS to CH	Not robust against on-off attack	minimal(Calculation and communication overhead)
HTMS Karthik et al., 2017)	Hybrid	An energy efficient attack resistant TMS	Weight	Communication data trust, data provenance, and interdependence property are considered in trust estimation	Not suitable for non-numeric data	Minimal
LTS (Khan et al., 2019)	Hybrid	Node behavior based Trust estimation,overhead reduction, Attack mitigation	Node behavior, weight, beta probability distribution function	Intra-cluster: CM to CM ,CH to CM Inter-cluster: CH to CH, BS to CH	Not robust against on-off attack	Minimal

The primary objective of the research is to reduce the communication overhead and memory overhead issues in the clustered wireless sensor network. There are several challenges during communication among SNs in WSN, such as data security, congestion, packet loss, and resource management. The proposed trust model is supposed to resolve the issue regarding security using TMS and advanced cryptographic approach. The proposed system would be capable to prevent greyhole attack, bad mouthing attack with the help of analyzing the consistency of trust values. In

this research work, we have considered Trust value range as [0, 4] to minimize memory overhead. Moreover, resource management in the proposed trust model has been performed using an optimal task-scheduling algorithm. It has been observed that nodes usually estimate trust value for other nodes with the help of a well-known mechanism known as a timing-window concept (Khan et al., 2019).

Proposed System

This section discussed a clustered architecture of sensor nodes (SNs) deployed in the targeted area as shown in figure 1.

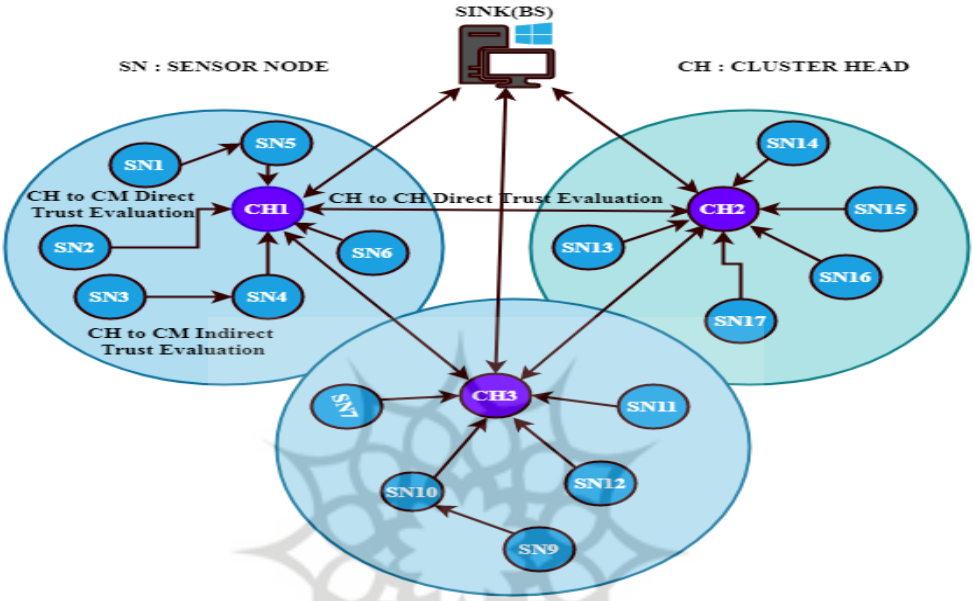

Figure 1.WSN Topology.

The proposed trust estimation approach is simple, effective and practical since it detects and eliminates the faulty data from the networks. It is attack resilient and trustworthy with less overhead due to task scheduling algorithm (Dai et al., 2011). Figure 2 shows the flow chart of the proposed work.

Intracluster Trust Evaluation

Trust calculation within a cluster (intracluster) is discussed in the following two subsections, namely CM to CM and CH to CM trust evaluation scheme respectively, to obtain an accurate and robust trust values.

CM to CM direct trust evaluation scheme

Within a cluster, communication trust and data trust $T_{x,y}(\Delta t)$ between CMs is computed using the Eq.(1) as follows.

$$T_{x,y}(\Delta t) = \left[4 \times \left(\frac{S_{x,y}(\Delta t)}{(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))}\right) * \frac{1}{\psi^{U_{x,y}(\Delta t)}} * \phi^{S_{x,y}(\Delta t)}\right] \quad (1)$$

Where $S_{x,y}(\Delta t)$ and $U_{x,y}(\Delta t)$ denote the number of successful interactions and unsuccessful interactions respectively during the time Δt.

Figure 2. Flow diagram

The first term $\left(\frac{S_{x,y}(\Delta t)}{(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))}\right)$ provide the ratio of successful interactions to the total interactions and second term $\frac{1}{\psi^{U_{x,y}(\Delta t)}}$ provide a flexible punishment to the malicious nodes where $the\ variable\ \psi$ can be tuned according to application requirement and network scenario. The third term $\phi^{S_{x,y}(\Delta t)}$ provides reward to good (genuine) nodes during successful interactions. In this model, punishment and reward can be adjusted according to application requirement takes makes it a novel, flexible and robust trust model. Successful data report between two SNs is estimated using (Khan et al., 2019) which is important to improve the accuracy of proposed Trust model.

CH to CM feedback (indirect) trust estimation ($FT_{x,y}(\Delta t)$)

When there are no interactions (successful and unsuccessful) among CMs then Cluster head collects direct trust values of (n-1) cluster members by periodically sending a request packet and store in an (n-1)* (n-1) matrix as follows:

$$CH = \begin{bmatrix} T_{1,1} & T_{1,2} & \dots & T_{1,n-1} \\ T_{2,1} & T_{2,2} & \dots & T_{2,n-1} \\ \dots & \dots & \dots & \dots \\ T_{n-1,1} & T_{n-1,2} & \dots & T_{n-1,n-1} \end{bmatrix}$$

Inspired from the beta distribution function (Li et al., 2013) (Singh et al., 2017), feedback trust can be estimated as follows using Eq. (2).

$$FT_{x,y}(\Delta t) = 4 * \frac{a+1}{a+b+2} \quad (2)$$

Where a and b are the amount of positive and negative feedbacks, respectively. A feedbacks is said to be positive if and $T_{x,y}(\Delta t) \geq 2$ and negative if$T_{x,y}(\Delta t) < 2$. Final trust value $(f_{x,y}^{T}(\Delta t))$ is computed by simply aggregating eq(1) and eq(2) (as simple averaging performs better than complex averaging (Ishmanov et al., 2015)) as follows using Eq. (3).

$$f_{x,y}^{T}(\Delta t) = \frac{T_{x,y}(\Delta t)+FT_{x,y}(\Delta t)}{2} \quad (3)$$

To find the node status, $FT_{x,y}(\Delta t)$component is used as follows

$$S\left(f_{x,y}^{T}(\Delta t)\right) = \begin{Bmatrix} (3;4) \\ (0;\theta) \\ (\theta;3) \end{Bmatrix} \begin{matrix} highly trusted node \\ malicious node \\ legitimate node \end{matrix}$$

The value of (or parameter) θ is application dependent i.e. ,its value can be tuned according to application requirements and network scenario.

Intercluster Trust Evaluation

Trust calculation at the intercluster level is also defined by CH-to-CH (direct) and BS to CH (indirect) trust calculation. CH-to-CH trust is calculated using Eq. (4) in the same way as at CM level, but during BS to CH trust calculation, BS discards the dishonest feedbacks and simply aggregate remaining feedbacks. Note that at inter-cluster level, we consider only communication trust (not data trust) because adjacent CHs aggregate the data coming from CMS, and it will be challenging to find the false (untrustworthy) data report from the aggregated data. Figure 3 shows the flowchart of trust evaluation at the intercluster level.

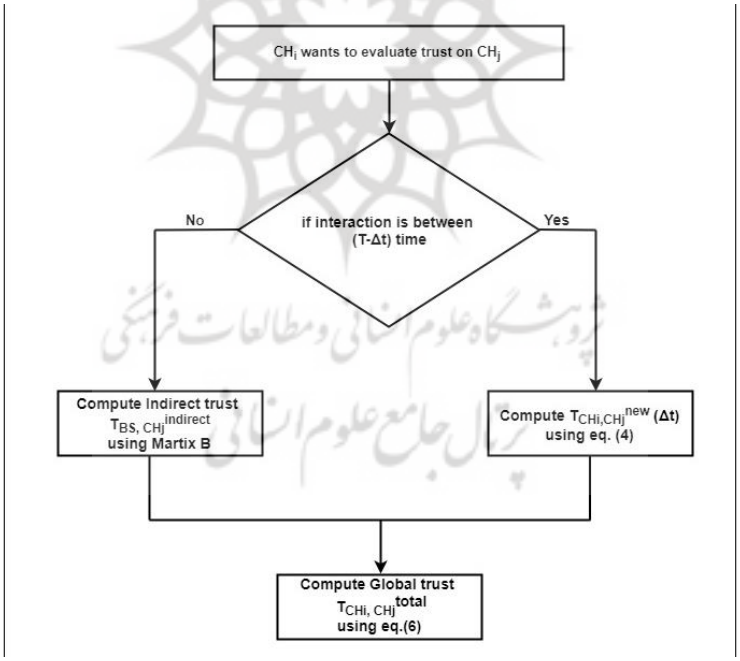

Figure 3. Trust calculation at the intercluster level

CH to CH Direct trust estimation

The direct trust estimation between CH_i and CH_j is defined as follows using Eq. (4).

$$T_{\mathrm{CH_i},CH_j}(\Delta t) = \left[4 \times \left(\frac{S_{\mathrm{CH_i},CH_j}(\Delta t)}{\left(S_{\mathrm{CH_i},CH_j}(\Delta t)+U_{\mathrm{CH_i},CH_j}(\Delta t)\right)}\right) * \frac{1}{\sqrt{U_{\mathrm{CH_i},CH_j}(\Delta t)+1}} * \phi^{S_{\mathrm{CH_i},CH_j}(\Delta t)}\right] \quad (4)$$

The first and third terms in Eq.(4) plays the same role as in Eq.(1). The second term is known as punishment factor (wrt. CHs) that give strict punishment with the increase in unsuccessful interactions. As we know that CHs are powerful and trusted node, unsuccessful interactions among CHs should decrease the trust value. We have intentionally added 1 with $U_{\mathrm{CH_i},CH_j}(\Delta t)$ to keep the trust value within the specified range. Consider the scenario when we have not added 1 with $U_{\mathrm{CH_i},CH_j}(\Delta t)$ and suppose the number of unsuccessful interactions between CH (i) and CH(j) is zero then the value of $\mathrm{T}_{\mathrm{CH_i},\mathrm{CH_j}}(\Delta t) = \infty$ that is non-realstic because trust value between any two entities never be infinite.

BS to CH feedback Trust calculation

To obtain CHs trust values, Base station periodically sends a request packet to cluster heads (suppose m) in the same fashion as cluster head sends to cluster members. In response to request packet, cluster heads forwards their direct trust values to the base station. To compute feedback trust value, the base station (BS) maintains these values into a matrix as follows

$$B = \begin{bmatrix} CH_{1,1} & CH_{1,2} & \dots & CH_{1,m} \\ CH_{2,1} & CH_{2,2} & \dots & CH_{2,m} \\ \dots & \dots & \dots & \dots \\ CH_{m,1} & CH_{n-1,2} & \dots & CH_{m,m} \end{bmatrix}$$

In the matrix B maintained at BS, the values $CH_{1,1}$ to $CH_{m,m}$ may be untrusthworthy recommeeedation which should be discared for correct trust decision at the base station. So during trust calculation, BS discard self recommeeedation to reduce the self boosting trust value because a malicious CH may send false trust value about itself to boost self trust value. Inspired by the beta distribution function, feedback trust can be estimated as follows using Eq. (5).

$$FT_{BS,CH_j}(\Delta t) = 4 * \frac{\mathrm{p}+1}{\mathrm{p}+b+2} \quad (5)$$

Where p is positive feedback and b is negative feedback. A global trust value ($G^T_{CH_i,CH_j}(\Delta t)$) can be obtained at CHs as follows using Eq. (6).

$$.(G^T_{CH_i,CH_j}(\Delta t)) = \frac{\mathrm{w}_1 * T_{\mathrm{CH_i},CH_j}(\Delta t) + \mathrm{w}_2 * FT_{BS,CH_j}(\Delta t)}{2} \quad (6)$$

Where w_1 and w_2 are respective weight-age and depending upon the application requirement, w_1 and w_2 will give more flexibility to select appropriate weight-age for the robust TMS.

Note: In the proposed model, the term P can be used to represent the percentage of successful interactions as follows using Eq. (7).

$$.P = \frac{s}{s+f} \quad (7)$$

Where s (or $\mathrm{s}_{\mathrm{x,y}}$) is the number of successful communication and f is the number of unsuccessful communication between sensor nodes x and y in one time unit of the time window. Similarly, the percentage of unsuccessful interactions (U) can be defined as follows using Eq. (8).

$$U = 1 - P \quad (8)$$

Authentication based Data Trust (ADT)

Let us suppose reward and penalty (in case of ADT) is $\mathrm{r}_{\mathrm{ADT}}$, and Penalty $\mathrm{p}_{\mathrm{ADT}}$ respectively then the value of P and U using Eq.(7) and Eq.(8) in terms of reward and punishment can be defined using Eq. (9) and Eq. (10) as follows

$$P_{ADT} = \frac{r_{ADT}}{r_{ADT+\, p_{ADT}}} \quad (9)$$

$$U_{ADT} = \frac{p_{ADT}}{r_{ADT+\, p_{ADT}}} \quad (10)$$

Scheduler based Node Trust (SNT)

Let us suppose reward and penalty (in case of SNT) is $r_{SNT,}$ and Penalty p_{SNT} respectively then the value of P and U in terms of reward and punishment can be defined using Eq.(11) and Eq.(12) as follows

$$P_{SNT} = \frac{r_{SNT}}{r_{SNT+\, p_{SNT}}} \quad (11)$$

$$U_{SNT} = \frac{p_{SNT}}{r_{SNT+\, p_{SNT}}} \quad (12)$$

Trust Decision based on Either ADT or SNT

Using Eq. (1), we can write authentication or scheduler based trust (T_{AOS}) as follows.

$$T_{AOS} = (T_{x,y}^{ADT}) + (T_{x,y}^{SNT}) \quad (13)$$

where $T_{x,y}^{ADT}$ and $T_{x,y}^{SNT}$ are the trust values for ADT and SNT computed using proposed eq (1) to obtain robust trust value.

Trust Decision based on ADT and SNT

Using Eq.(1), we can write authentication or scheduler based trust (T_{AOS}) as follows

$$T_{AAS} = (T_{x,y}^{ADT}) * (T_{x,y}^{SNT}) \quad (14)$$

Overhead Analysis

This section discussed the comparative analysis of the various state of the art TMS. Table 2 provides the communication overhead, and Table 3 presents a comparison of the different trust models.

Table 2. Communication Overhead Analysis

Trust management Scheme	**Total Communication Overhead**
(Ganeriwal et al., 2008)	2*g[n*(n-2)*(n-1)+(g-1)*(g-2)]
(Yao et al., 2006)	$2*g[n\ (n-1)^2 + (g-1)^2]$
(Boukerche et al., 2007)	4g[n(n-1)+ (g-1)]
(Zhang et al., 2010)	$constant\ i.e$ independent of n amd g
Shaikh et al., 2008)	2g[n(n-1)*r+(n-1)]
(Li et al., 2013)	$2g[(n-2)(n-1)+n]+2\ (g-1)^2 + 2g$
(Talbi et al., 2017)	$2g\ (n-1)^2+2(g)^2$
(Singh et al., 2017)	$g[(n)^2(n-1)+g(g-1)]$
(Khan et al., 2019)	g*(2 (n-2)(n-1)+ 2r)+2g(g-1)+ 2g
proposed approach	Equal to LTS (Khan et al., 2019)

Table 3. Comparison of WSN Trust functions

Trust management Scheme	Observation	Trust function
(Zhang et al., 2010)	Only communication trust	$\frac{S}{S+U}$
Shaikh et al., 2008)	Only communication trust	$\frac{S^2}{(S+U)*(s+1)}$
(Li et al., 2013)	Only communication trust	$\frac{S}{S+U} * \frac{1}{\sqrt{U}}$
(Talbi et al., 2017)	Communication and Data trust	$\frac{S}{S+U}^{(1-\frac{S}{S+U})\alpha}$
(Singh et al., 2017)	Only communication trust	$\frac{(S^{G1}+S^{G2})}{(S^{G1}+S^{G2}+U^{G1}+U^{G2})} * \frac{1}{\sqrt{P1*U^{G1}+P2*U^{G2}}} * (\frac{p1*S^{G1}+p2*S^{G2}}{1+p1*S^{G1}+p2*S^{G2}})$
(Khan et al., 2019)	Communication and Data trust with flexible punishment coefficient	$(\frac{S}{S+U})^* (\frac{1}{\psi^U})^* (\frac{S}{S+1}^{\alpha})$ where α is exponent to $\frac{S}{S+1}$
proposed approach	More flexible, Realistic, Adaptive and Dynamic	$4 \times \left(\frac{S_{x,y}(\Delta t)}{(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))}\right) * \frac{1}{\psi^{U_{x,y}(\Delta t)}} * \phi^{S_{x,y}(\Delta t)}$

Result

Since it is already proved in (Khan et al., 2019) that ADCT (Talbi et al., 2017) is better than GTMS (Shaikh et al., 2008), TMA (Zhang et al., 2010), LDTS (Li et al., 2013) in terms of attack mitigation, communication overhead and memory overhead so we are comparing our proposed work with ADCT (Talbi et al., 2017) by considering parameter values in the same proportion for better comparative analysis. In tradition work, reward and penalty are 0.5. The value of P was calculated as P=reward / (reward + penalty). Table 4 had been generated according to the parameter (a orα) to analyze the severity of the trust model. Figure 4 is plotting in MATLAB with the corresponding data provided in table 5.

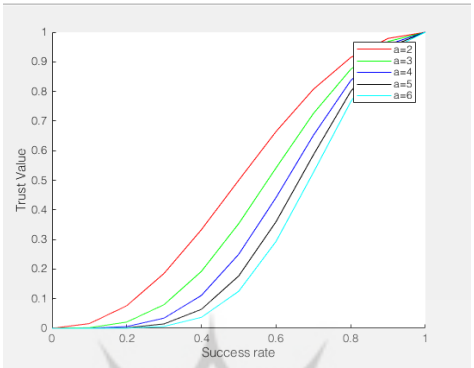

Figure 4. Graph representing trust value in ADCT (Talbi et al., 2017)

Table 4. Variation of trust values wrt. a (or α).

P	a=2	a=3	a=4	a=5	a=6
0	0	0	0	0	0
0.1	0.0158	0.002	0.0003	0	0
0.2	0.0761	0.021	0.0058	0.0016	0.0004
0.3	0.1853	0.0798	0.0344	0.0148	0.0064
0.4	0.333	0.1922	0.1109	0.064	0.0369
0.5	0.5	0.3536	0.25	0.1768	0.125
0.6	0.6645	0.5417	0.4416	0.36	0.2935
0.7	0.8073	0.7254	0.6518	0.5857	0.5262
0.8	0.9146	0.8747	0.8365	0.8	0.7651
0.9	0.9791	0.9689	0.9587	0.9487	0.9387
1	1	1	1	1	1

Case 1. Comparing trust model with (strong penalty) and where (reward and penalty are equal)

In case 1 of the proposed work, the Trust values were calculated using Eq.(1) and Eq. (7). They used 0.4 as reward and 0.6 as a penalty. The value of P was calculated as P=reward / (reward penalty). Table 4 had been generated according to the different parameter of severity and shows the variation in trust values with the change in α. Moreover, Table 5 indicates the decrease in trust value which in turn indicate the robustness of trust model because of lesser the trust value with increased no. of interaction, more robust and attack resistant trust model. Note that trust value should not increase rapidly with increased no. of successful interactions.

Table 5. Trust values generated in case (1)

a (or α) values	2	3	4	5	6
Equal reward and penalty – E	0.5	0.3536	0.25	0.176	0.125
Strong penalty small reward – S	0.333	0.1922	0.110	0.064	0.036
E-S	0.167	0.1614	0.139	0.112	0.088

Similarly, table 6 and table 7 indicate the robustness, accuracy, and attack detection capability of the trust model.

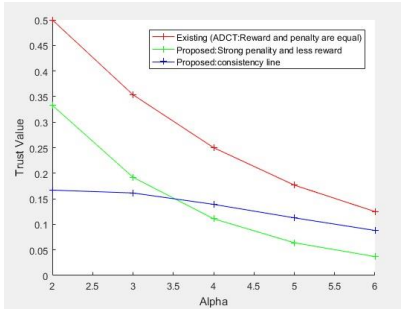

Figure 5: Comparing trust model with strong penalty with existing model (ADCT (Talbi et al., 2017))

We have "compared proposed work with an existing approach ADCT (Talbi et al., 2017) using MATLAB, as shown in fig.5. In ADCT (Talbi et al., 2017), Alpha (α or a) has been considered as a parameter to provide the severity of trust function. The experimental result shows that our approach is far better than the existing method in terms of malicious node detection and persistence of malicious behavior. We have analyzed the consistency of trust values with the change in α value. The consistency line (in figure 5) shows that trust values are changing slowly that indicates the accuracy of the trust model because a good trust model should avoid rapid increase or decrease in trust values."

Case 2.Integration of Trust Equation for ADT along with SNT

In case (2) of proposed work, the Trust values were calculated using Eq. (14) that has been derived from Eq. (1) and Eq. (9). We have used 0.4 as reward and 0.6 as a penalty. Here authentication mechanism and scheduling (Nasser et al., 2013) both simultaneously used to improve the performance of proposed TMS.

Table 6. Trust values generated in case 2

a (or α) values	2	3	4	5	6
Variation in trust values [31]	0.333	0.1922	0.1109	0.064	0.0369
Proposed Trust model with Scheduling and security	0.0369	0.0071	0.0014	0.0003	0.0001

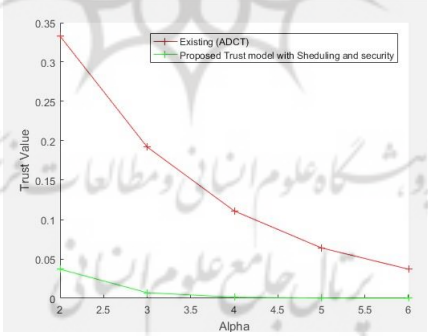

Fig. 6: Comparing trust model with Integration of Trust Equation for ADT and SNT

Table 6 had been generated in MATLAB according to the different parameter of severity (α). This scenario represents the effect of Integration of trust equation for ADT along with SNT. Figure 6 provides a comparative analysis of change in trust values. This approach reduces suddenly increase in trust values by various selfish nodes.

Case 3. Integration of either ADT or SNT.

In case (3) of proposed work, the Trust value was calculated using Eq. (13) that has been derived from Eq.(1) and Eq.(11). We have used 0.4 as reward and 0.6 as a penalty. Table 7 had been generated in MATLAB according to the different parameter of severity.

Table 7. Trust values generated in case 3

a (or α) values	2	3	4	5	6
Existing[31] Trust model	0.333	0.1922	0.1109	0.064	0.0369
Trust model with Scheduling or security	0.2218	0.0739	0.0246	0.008	0.0027

This case represents the effect of using either Integration of Trust Equation for Authentication based Data or Trust along with Scheduler based Node Trust. Figure 7 depicts the variation in trust values when authentication or scheduling is integrated with the trust model. This approach provides adaptability in the reduction of communication overhead (due to scheduling) or making it attack resilient (due to ADT). The word "or" plays a significant role as it covers either the first case or second case or both.

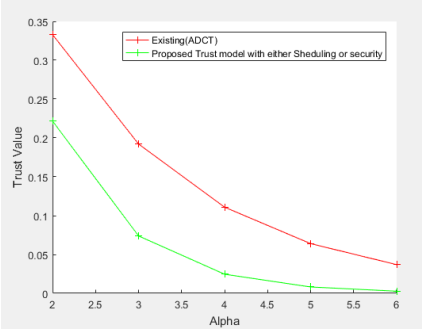

Fig.7. Comparing the trust model with Integration of Trust Equation for ADT or SNT

Conclusion

The proposed hybrid trust estimation approach for large scale WSN employing clustering to improve cooperation, trustworthiness, and security by detecting selfish sensor nodes with reduced resource (memory, power) consumption. The proposed scheme consists of unique features like authentication based data trust, scheduler based node trust, and attack resistant by giving the high penalty and minimum reward during node misbehavior. A task scheduling mechanism is employed for scheduling the significant task to reduce computation overhead. The proposed trust model would be capable to provide security against blackhole attack, grey hole attack, and badmouthing attack. Moreover, the proposed trust model feasibility has been tested with MATLAB. Simulation results exhibit the great performance of our proposed approach in terms of trust evaluation cost, prevention, and detection of malicious nodes with the help of analyzing consistency in trust values and communication overhead.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Boukerch, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, *30*(11-12), 2413-2427.

Basan, A., Basan, E., & Makarevich, O. (2016, October). Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust. In *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 409-412). IEEE.

He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE transactions on information technology in biomedicine*, *16*(4), 623-632.

Crosby, G. V., Pissinou, N., & Gadze, J. (2006, April). 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* (pp. 10-pp). IEEE.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *4*(3), 1-37.

Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2014). An efficient distributed trust model for wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *26*(5), 1228-1237.

Ishmanov, F., Malik, A. S., Kim, S. W., & Begalov, B. (2015). Trust management system in wireless sensor networks: design considerations and research challenges. *Transactions on Emerging Telecommunications Technologies*, *26*(2), 107-130.

Jadidoleslamy, H., Aref, M. R., & Bahramgiri, H. (2016). A fuzzy fully distributed trust management system in wireless sensor networks. *AEU-International Journal of Electronics and Communications*, *70*(1), 40-49.

Tan, S., Li, X., & Dong, Q. (2015). A trust management system for securing data plane of ad-hoc networks. *IEEE Transactions on Vehicular Technology*, *65*(9), 7579-7592.

Zhou, Y., Huang, T., & Wang, W. (2009, September). A trust establishment scheme for cluster-based sensor networks. In *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-4). IEEE.

Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. *Sensors*, *11*(2), 1345-1360.

Liu, Z., Zhang, Z., Liu, S., Ke, Y., & Chen, J. (2011, September). A trust model based on Bayes theorem in WSNs. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-4). IEEE.

Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2008). Group-based trust management scheme for clustered wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *20*(11), 1698-1712.

Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE transactions on network and service management*, *9*(2), 169-183.

Li, X., Zhou, F., & Du, J. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE transactions on information forensics and security*, *8*(6), 924-935.

Zhang, B., Huang, Z., & Xiang, Y. (2014). A novel multiple-level trust management framework for wireless sensor networks. *Computer Networks*, *72*, 45-61.

Ishmanov, F., Kim, S. W., & Nam, S. Y. (2015). A robust trust establishment scheme for wireless sensor networks. *Sensors*, *15*(3), 7040-7061.

Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2014). An efficient distributed trust model for wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *26*(5), 1228-1237.

Won, J., & Bertino, E. (2015, November). Distance-based trustworthiness assessment for sensors in wireless sensor networks. In *International conference on network and system security* (pp. 18-31). Springer, Cham.

Talbi, S., Koudil, M., Bouabdallah, A., & Benatchba, K. (2017). Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. *Telecommunication Systems*, *65*(4), 605-619.

Dogan, G., & Avincan, K. (2017). MultiProTru: A kalman filtering based trust architecture for two-hop wireless sensor networks. *Peer-to-Peer Networking and Applications*, *10*(1), 278-291.

Singh, M., Sardar, A. R., Majumder, K., & Sarkar, S. K. (2017). A lightweight trust mechanism and overhead analysis for clustered WSN. *IETE Journal of research*, *63*(3), 297-308.

Karthik, N., & Ananthanarayana, V. S. (2017). A hybrid trust management scheme for wireless sensor networks. *Wireless Personal Communications*, *97*(4), 5137-5170.

Khan, T., Singh, K., Abdel-Basset, M., Long, H. V., Singh, S. P., & Manjul, M. (2019). A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *Ieee Access*, *7*, 58221-58240.

Dai, L., Chang, Y., & Shen, Z. (2011). An optimal task scheduling algorithm in wireless sensor networks. *International Journal of Computers Communications & Control*, *6*(1), 101-112.

Yao, Z., Kim, D., & Doh, Y. (2006, October). PLUS: Parameterized and localized trust management scheme for sensor networks security. In *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems* (pp. 437-446). IEEE.

Zhang, J., Shankaran, R., Mehmet, A. O., Varadharajan, V., & Sattar, A. (2010, October). A trust management architecture for hierarchical wireless sensor networks. In *IEEE Local Computer Network Conference* (pp. 264-267). IEEE.

Nasser, N., Karim, L., & Taleb, T. (2013). Dynamic multilevel priority packet scheduling scheme for wireless sensor network. *IEEE transactions on wireless communications*, *12*(4), 1448-1459.

Bibliographic information of this paper for citing:

Khan, Tayyab; Singh, Karan; Gupta, Sakshi&Manjul, Manisha (2022).Multi Trust-based Secure Trust Model for WSN.*Journal of Information Technology Management*, Special Issue,147-158.