



PDTB-IDS: A Parameter and Distributed Trust Based Intrusion Detection System for Wireless Sensor Network

Shobha Aswal,

Asst. Professor, School of Computing, Graphic Era Hill University,
Dehradun, Uttarakhand India 248002

Abstract:

Techniques used in cryptography can provide authentication, confidentiality, and integrity. Wireless sensor networks must, however, also defend against both internal and external intruders. Many researchers in the field of wireless sensor networks recommend the use of a trust management system to combat assaults from malicious or compromised nodes as well as from outside attackers. Security management applications like secure data aggregation, secure cluster head selection, trusted routing, access control, etc. can all benefit from the implementation of trust management systems. Numerous researchers offer a variety of trust management-based solutions for these safe applications. However, it is necessary to build and construct a trust management system that takes into account numerous elements and applications of wireless sensor networks in order to integrate all such applications on a single sensor node in the network. Afterwards, the sensor hub's overall trust estimate is assessed by combining the separate trust esteems for the components' coordinate trust, proposal trust, and circuit trust. Indicators of trust obtained from the suggested method can be used by the trust model to determine if a certain hub is harmful or not. Using the NS2 simulation environment, the research's numerical evaluation is finished, and it is demonstrated that the projected technique yields better results than the current TSSRM method.

Keywords: Wireless Sensor Network, Security, Parameter, and Trust Factors, Intrusion Detection.

DOI Number: 10.48047/nq.2022.20.8.NQ221056

NeuroQuantology2022;20(8): 10358-10363

INTRODUCTION

A new invention called the Wireless Sensor Network (WSN) sends a number of small hubs out into the open to detect numerous marvels [1]. The use of cryptography can ensure validity, classification, and integrity. However, experts propose a hope-related structure to deal with outer assaults like dark gaps, sinkholes, and Denial of Service (DOS) attacks. Trust boards have produced excellent results in other system domains, such as unofficial groups, impromptu systems, and P2P systems. As WSN is an asset requirement arranges, the usual technique

and methods that are important to various systems are not directly applicable to remote sensing systems. If the hub executes each operation in accordance with the unique standards of systems administration, the hope between hubs will increase. In the unlikely event that a hub violates the system's rules, it must be identified as a malignant hub and removed from future system communication. The hub will build a relationship of trust based on its quick assessment and advice. In any event, as the topology of hubs changes dramatically, these proposal frameworks become



increasingly valuable. The expansion of correspondence costs will result from the exchanging of proposal data in a secure manner. For instance, zero represents complete doubt, whereas one represents complete confidence. Hope is the typical possibility of conviction, and actual likelihood is confirmed to be trustworthy. Errors in expectation and dependability classification will give room for shaky judgment of effects. Sometimes trust isn't enough to complete a mission. But before they are included in the hope calculation, risk, value of service, and hope should be controlled separately. However, the hope board structure must affect various forms of usage in each level of the convention stack. Most of the time, the executive's framework for examining trust just considers a few criteria and trust-related factors. A hope the executives system should take into account a variety of variables and hope elements connected with hubs in a distant sensor arrange. Every detector hub in a hope system needs to keep an eye on its neighbor while supporting numerous metrics. The characteristics of a nearby hub are guaranteed by the combined estimation of these hope factors. These perspectives are taken into account when creating a trust board framework in the structure proposed in this study. This strategy is appropriate for systems at the group and plane levels.

The pursuits below describe the exploratory work's most important commitments:

1. PDTB-IDS is suggested as a way to identify malicious hubs in a clustered WSN. The approach suggested in this article examines two perspectives for constructing a trust the board framework.

The immediate experience and encounters with the adjacent hubs of the checked hub are used to determine the deviation. Second, each sensor hub should monitor its neighbor, supported by various parameters such as packets sent, communicated, and so on. Supported by these monitored parameters, the trust variables are evaluated. The dependability of a neighbor hub is ensured by the combined evaluation of those trust components.

2. The overall trust estimation of an SN is then calculated by adding the individual hope estimations from each level. The hope value is then transferred to the Cluster Head (CH) at that time. At that moment, the CH uses limited reverence to determine whether the SN is real or harmful. This trust worth is updated every so often.

RELATED WORK

Different models for hope-related protected correspondence were predicted by the experts for various sorts of systems, including informal organizations, unrehearsed systems, peer-to-peer networks, and distant detector systems. FarruhA clear understanding of the hope executive's framework in remote sensor systems is provided by Ishmanov et al. [2]. They have looked into the value of trust managers in distant detection systems as well as considered several types of trust techniques. The trust framework for remote sensor systems is still in its infancy and needs additional improvement from a range of viewpoints because remote detector systems are still a relatively new field. As a result, the trust board framework generally plays a big role in providing secure communication. To effectively manage narrow-minded or harmful hubs, Fenyé et al. presented a progressive trust executive convention based on a highly adaptable group for WSN [3]. The evaluation of trust depends on a variety of factors.

An occasion-related hope board system was presented by Chen et al. [4]. The estimation of hope is dependent on the certainty and event. The system's designers used the fuzzy hypothesis notion to determine the trust level [5]. A hope assessment calculation (NBBTE) was anticipated by Feng et al. in light of the banded conviction hypothesis [6].

Our method focuses on attacks that deliberately attempt to skip vital node-to-node communication. Insider assaults when an intruder is able to compromise the routing capabilities of devices, are one method for doing this in ad-hoc networks. [7]. To build a strong trust the board plot, Luo et al. used behavior names for the sensor hubs [8]. The authors of [9] used the weighting approach for trust calculating and evaluation. Ishmanov et al. calculated the weight period of a hub's negative



behavior to identify malicious hubs in the system[10]. By using weighting parameters and quantifiable procedures, Bao et al. reduced the false-positive rate and projected a hope strategy for WSN [11]. For grouped WSN, Zhang et al. projected a hope model that was dependent on the cloud model [12].

A flexible trust-based affirmation IDS employing dynamic fruitful conveyances was developed by Rajesh kumar et al. [13]. This technique makes use of the Kalman channel to evaluate a hub's trustworthiness. A physical layer IDS was put forth in [14] to provide protection at the physical layer. This method only pinpoints the refusal of an administration attack brought on by a sticking attack.

It is clear from the literature reviewed above that using appropriate trust metrics to determine an SN's level of trust is crucial. Therefore, it is important to monitor node behaviour when creating an IDS. In this work, we have chosen the appropriate trust metrics for calculating trust at each tier and have identified a node's behaviour in response to an attack. As far as we know, not much work has been done to develop a protocol layer trust-based IDS in this domain.

In this study, the trust is estimated at each tier by taking the trust metrics' deviance into account, a sensor node's total trustworthiness is calculated by averaging the individual trust levels.

IDS based on PARAMETER AND DISTRIBUTED TRUST

We presuppose a cognitive WSN in which a smart SN has the ability to dynamically alter its behaviour in response to both internal and external factors. Even if it is not inherently compromised, an SN may become uncooperative in order to conserve energy. Sensing functions are frequently stopped and communications are randomly dropped as a result of the uncooperative behaviour. If not compromised, an uncooperative SN may turn cooperative to support system objectives like service availability if there aren't many cooperative neighbour nodes present. Low energy (since a node with high energy may perform stronger energy-intensive defences against attackers) or more compromised neighbours nearby increase the

likelihood that an SN will be compromised. A compromised SN is capable of both strong attacks, such as black hole attacks, godmouthing attacks (which recommend a bad node as a good node) and badmouthing attacks (which recommend a good node as a bad node), which cause it to act dishonestly, and weak attacks, such as message dropping and selective packet forwarding, which cause it to act uncooperatively.

A SN or CH will require more energy to carry out attacks once it has been compromised. These assault behaviours act as indicators that the trust characteristics of honesty, energy, and cooperation are lacking.

3.1 Network Model:An organized WSN makes up the structure model. In the system, a group has a CH and SNs. The SNs use remote correspondence to communicate with one another. SNs can legitimately communicate with base stations (BS) through remote communication or indirectly through other SNs.

Attackers primarily alter routing information at the network layer by disseminating false information like the minimum hop count. We have taken the sinkhole attack into consideration in this effort. In this attack, the malicious node broadcasts false routing information, such as a low hop count, in regular updates. We assume that during route discovery using the Ad hoc On Demand Distance Vector routing protocol (AODV), the node communicates the low hop count information in the route reply packet (RREP). Therefore, it's important to find the sinkhole assault. The hop count (hp) parameter is used as an IDS in this layer to find rogue nodes in the network. By accumulating each individual hope at every level, the general trust of SN is established. The CH is then sent the SN's overall hope estimation at that point. The CH uses the thresholding scheme to determine whether the SN is malicious or genuine.

3.2. Metrics for Parameters: A hub i must keep an eye on its neighboring hub j in order to calculate trust between two hubs. E is recorded on the system each time. Where there were six distinct informational gatherings that might be viewed on the system.

- Cryptographic Correctness



- Recommendation
- Energy
- Communication
- Location
- Data

Communication: The hub J keeps an eye on the hub I for all situations related to communication. The following are the parameters associated with correspondence:

- a) PS- Number of packets sent
- b) PR- Number of packets received
- c) PF- Number of parcels forwarded
- d) PCS- Number of control packets sent
- e) PCR- Number of control packets received
- f) PB- Number of broadcast packets received
- g) PDS- Number of data packets sent
- h) PDR - Number of data packets received

Data: The sensor hub may pick up media information as well as static data. The information regarding the information needs to be stored for future planning. The recommendation given by adjacent hubs can also be taken as information in the event that the trust executives employ ad hoc trust.

Suggestion: The hub's neighbor hub's behavior with regard to sending ideas is shown by the amount of proposal data that is sent, received, and displayed. Area: The majority of steering conventions take into account directing based on geographical area. A hub's area data can be false.

Strength: As the hubs are asset limitations, energy is one of the fundamental components of a remote sensor network.

Cryptographic accuracy: These elements are used to determine whether a system hub is behaving as it should, as suggested by cryptographic rules.

3.3 Trust-Management Factors

Evaluation of the reasons for hope influences the determination of a neighboring hub's optimism. Every reason for hope is evaluated based on factors that are observed. Seven reasons for optimism were identified, the majority of which had an impact on a hub's trust. Every trust factor is a component of several different parameters.

- a) Communication Trust
- b) Trust Update Time
- c) Energy Trust

- d) Functionality Trust
- e) Location Trust

3.4 Trust Model

Utilising trust models built on a variety of speculative concepts, trust elements are assessed. The weighted mean, the Bayesian model, the abstract rationale, the entropy-based model, the fuzzy reasoning-based model, the game-theoretic based model, the human hope technique, and bio-enlivened models are among the trust models that are most frequently employed.

3.5 Trust Building in WSN

Several different remote sensing system implementations can make use of the framework for the faith executive.

RESULTS AND DISCUSSION

The simulation result is determined by keeping the area size at 100 × 100 m2 on either side.

10361

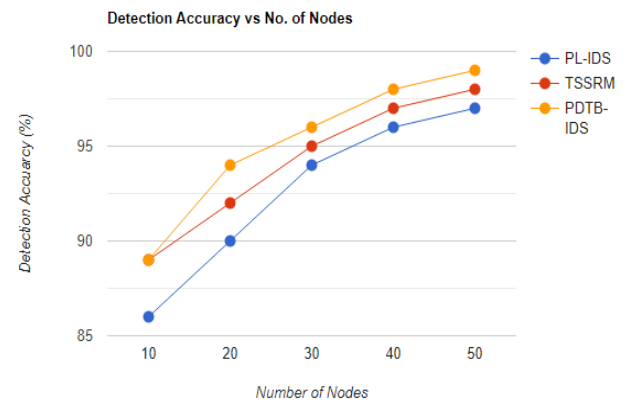


Fig. 1. Detection Accuracy vs No. of Nodes
 Through simulation, we also learn that a single selected forward attack may attempt to make a packet that has been received sink through its probability.

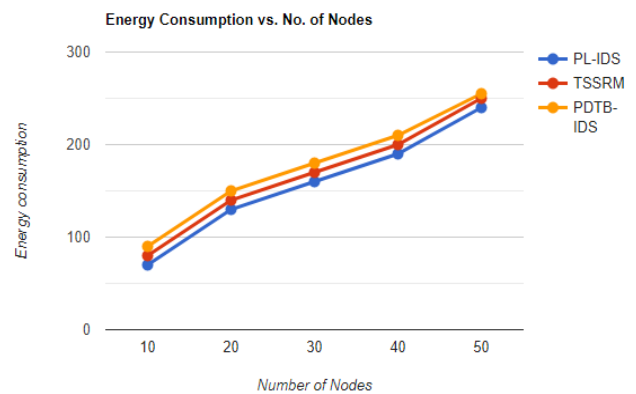


Fig. 2. Energy Consumption vs No. of Nodes



Information sneaky attack is a type of attack in which a hub delivers values to the Cluster head that are either unusually large or too instead of the actual value that was discovered. Several requirements are used to evaluate the anticipated approaches' performance. The effectiveness of LB-IDS is assessed by contrasting its performance with Wang's scheme in terms of detection accuracy, false-positive rate (FPR), and false-negative rate (FNR). The accuracy of the IDS's detection of malicious nodes is determined by detection accuracy. The detection accuracy is calculated at what ratio is true or false using FPR and FNR. The use of MATLAB R2015a is utilised when running computer simulations. The simulation is run on a computer with a core i7 processor, 6 GB of RAM, and a Windows 10 operating system. The most recent Wang et al. [1] system, which is similarly founded on protocol layer trust, is contrasted with the LB-IDS scheme.

The simulation's performance metrics are determined as follows:

- (1) Detection accuracy: the proportion of malicious SNs discovered among all malicious SNs in the network.
- (2) False-positive rate (FPR): the proportion of real SNs that were mistakenly identified as malicious.
- (3) False-negative rate (FNR): the proportion of malicious SNs out of all malicious SNs that are falsely identified as legitimate.

CONCLUSION

In terms of identifying malicious behavior, trust models have proven to be genuinely important. -e suggested Through the physical layer, MAC layer, and network layer detection of the jamming attack, back-off manipulation attack, sinkhole attack, and cross-layer attack, LB-IDS secures the WSN. In order to distinguish between legitimate nodes and malicious nodes in the network, trust threshold values at each tier are used. According to the findings, the LB-IDS scheme outperforms Wang et al. [1]'s in terms of detection accuracy, false-positive rate, and false-negative rate. In terms of message complexity, memory overhead, energy usage, and trust assessment, -e analysis for LB-IDS is also carried out. For the clustered WSN, LB-IDS will be a better security option. In the future, we'll use

wireless transceiver modules placed outside to implement and evaluate the suggested LB-IDS. The calculations of direct trust, suggestion, trust, and aberrant trust have been explored. The results show that PDTB-IDS outperforms PL-IDS and TSSRM conspire in terms of recognition accuracy, throughput, energy utilization, and other factors. It has been noted that the suggested PDTB-IDS will become a more reliable security solution for the grouped WSN. The goal for the coming work is to fully implement this methodology in various trust applications.

REFERENCES

- [1] 1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) Wireless Sensor Networks: A Survey. *Computer Networks*, 38, 393-422.
- [2] Ishmanov, F., Malik, A.S., Kim, S.W. and Begalov, B. (2013) Trust Management System in Wireless Sensor Networks: Design Considerations and Research Challenges. *Transactions on Emerging Telecommunications Technologies*
- [3] Bao, F.Y., Chen, I.-R., Chang, M.J. and 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, 169-183.
- [4] Chen, H.G., Wu, H.F., Hu, J.C. and Gao, C.S. (2008) Event-Based Trust Framework Model in Wireless Sensor Networks. *Proceedings of International Conference on Networking, Architecture, and Storage*, 359-364.
- [5] N. Shao, Z. Zhou, and Z. Sun, "A lightweight and dependable trust model for clustered wireless sensor networks," in *Lecture Notes in Computer Science*, pp. 157-168, Springer, Berlin, Germany, 2016.
- [6] 6. R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345-1360, 2011.
- [7] R. Wu, X. Deng, R. Lu, and X. Shen, "Trust-based anomaly detection in wireless sensor networks," in *Proceedings of 2012 1st IEEE International Conference on Communications in*



- China (ICCC), pp. 203–207, Beijing, China, August 2012.
- [8] W. Luo, W. Ma, and Q. Gao, “A dynamic trust management system for wireless sensor networks,” *Security and Communication Networks*, vol. 9, no. 7, pp. 613–621, 2015.
- [9] X. Li, F. Zhou, and J. Du, “LDTS: a lightweight and dependable trust system for clustered wireless sensor networks,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.
- [10] F. Ishmanov, S. Kim, and S. Nam, “A robust trust establishment scheme for wireless sensor networks,” *Sensors*, vol. 15, no. 3, pp. 7040–7061, 2015.
- [11] F. Bao, R. Chen, M.J. Chang, and J.-H. Cho, “Trust-based intrusion detection in wireless sensor networks,” in *Proceedings of 2011 IEEE International Conference on Communications (ICC)*, pp. 1–6, Kyoto, Japan, June 2011.
- [12] T. Zhang, L. Yan, and Y. Yang, “Trust evaluation method for clustered wireless sensor networks based on cloud model,” *Wireless Networks*, vol. 24, no. 3, pp. 777–797, 2016.
- [13] G. Rajeshkumar and K. R. Valluvan, “An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network,” *Wireless Personal Communications*, vol. 94, no. 4, pp. 1993–2007, 2016.
- [14] U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, and S. K. Panda, “PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks,” *International Journal of Information Technology*, vol. 10, no. 4, pp. 489–494, 2018.
- [15] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, (2008) ReputationBased Framework for High Integrity Sensor Networks. *ACM Transactions on Sensor Networks*, 4, 1-37.
- [16] V. Geetha, and K. Chandrasekaran, (2013) Enhanced Beta Trust Model for Identifying Insider Attacks in Wireless Sensor Networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 13, 14-19.

