SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 299–307

ISSN No: 2454-9614

Trust Based Distributed Systems for Wireless Sensors Network

V. Ashwathi S. Karthikaveni *

Department Of Computer Science and Engineering, Surya Engineering College, Erode, Tamilnadu, India.

*Corresponding Author: V. Ashwathi

E-mail: aswathibe@gmail.com

Received: 12/11/2015, Revised: 15/12/2015 and Accepted: 10/03/2016

Abstract

These days trust models are a standout amongst the most essential to develop trust connections among sensor hubs. A large portion of the current work is feeling the loss of the accompanying issue. To start with issue is in the ebb and flow research work, the evaluation of trust qualities for sensor hubs is fundamentally taking into account the correspondence (fruitful and unsuccessful interchanges) perspective. The other trust measurements, for example, the vitality level ought to additionally be considered to compute the reliability of sensor hubs. Second there are two normal approaches to set up trust in WSNs: figuring direct trust in light of directs cooperation's and ascertaining circuitous trust esteem in view of proposal from the outsider. However, not all the outsiders are trusty and not every one of the proposals are solid. In this way, a separate investigation about the outsider and proposal is crucial. Third most existing concentrates just give the trust appraisal to neighbour hubs. In any case, in genuine applications, a sensor hub at times needs to acquire the trust estimation of the non-neighbour hubs. In this way, giving the trust evaluation to non-neighbour hubs turns out to be critical. Fourth, as a result of the dynamic topology, the trust relationship between sensors hubs always shows signs of change in WSNs. Trust are a dynamic wonder and changes with time and environment conditions. In any case, most existing trust models don't tackle the trust dynamic issue. So as to take care of the aforementioned issues, propose an Efficient Distributed Trust Model (EDTM) for WSNs. Usage results will demonstrate that EDTM beats other comparative models, e.g., (Node Behavioural procedures banding conviction hypothesis of the Trust Evaluation) NBBTE trust model.

Reviewed by* **ICETSET'16 *organizing committee*

Keywords: Wireless sensor networks, Distributed trust calculation, Energy efficient.

1. Introduction

In remote sensor systems different security components, e.g., cryptography, authentication, confidentiality and message integrity, have been proposed to avoid security threads such as eavesdropping, message replay, and fabrication of messages. Notwithstanding, these methodologies still experience the ill effects of numerous security vulnerabilities, for example, node capture attacks and Denial of Service (DoS) assaults. The conventional security components can oppose outer assaults, however can't understand inward assaults viably which are brought about by the caught hubs. To set up secure interchanges, we have to guarantee that all conveying hubs are trusted. This highlights the way that it is basic to set up a trust model permitting a sensor hub to surmise the reliability of another hub. It is unravelled in our proposed model Efficient Distributed Trust Model (EDTM**) [1].**

Presently, numerous inquires about have created trust models to fabricate trust connections among sensor systems [1].For example **[2],** a distributed Reputation-based Framework for Sensor Networks (RFSN) is initially proposed for WSNs. Two key building pieces of RFSN are Watchdog and Reputation System. Watch dog is in charge of observing correspondence practices of neighbour hubs. Reputation System is in charge of keeping up the notoriety of a sensor hub. The trust quality is figured in view of the Reputation value. However, in RFSN, just the immediate trust is ascertained while the proposal trust is overlooked. A parameterized and localized trust management Scheme (PLUS) is proposed in **[3].** In PLUS, both personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. Whenever a judge node (the node which performs trust evaluation) receives a packet from suspect node (the node which is in radio range of the judge node and will be evaluated), it always check the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviours or not. Therefore, suspect node may get unfair penalty. A Node behavioural strategy banding belief theory of the trust evaluation algorithm (NBBTE) algorithm is proposed based on the communication behaviour strategy banding D-S belief theory **[4].**NBBTE algorithm first establishes various trust factors depending on the communication behaviours between two neighbour nodes. Then, it applies the fuzzy set theory to measure the direct trust values of sensor nodes. Finally, considering the recommendation of neighbour nodes, D-S evidence theory method is adopted to obtain integrated trust value instead of simple weighted-average one. To the best of our knowledge, NBBTE is the first proposed algorithm which establishes various trust factors depending on the communication behaviours to evaluate the trustworthiness of sensor nodes. Localization algorithm with a mobile anchor based on triangular in WSNs (LMAT) is proposed in **[5].**Most existing studies only provide the trust assessment for neighbour nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbour nodes. In some routing protocols sensor nodes need the information of the two-hop neighbour nodes to establish the routing or localize themselves. Therefore, providing the trust assessment for non-neighbour nodes becomes very important so in this paper consider trust assessment for non-neighbour nodes. The provenance and value similarity is proposed in **[6].**Use two types of similarity functions: value similarity inferred from data values, and provenance similarity inferred from data provenances. Value similarity is based on the principle that the more data items referring to the same real-world event have similar values, the higher the trust scores of these items. We in this manner propose al methodology for figuring trust scores taking into account esteem closeness under the circulation of gathered information. Provenance likeness depends on the perception that diverse provenances of comparable information qualities might build the reliability of information things.

Trust Models have been as of late recommended as a compelling security system for Wireless Sensor Networks (WSNs). Extensive examination has been done on displaying trust. However, most ebb and flow research work just considers correspondence conduct to compute sensor hubs' trust esteem, which is insufficient for trust assessment because of the wide spreading malicious attacks.

1) In the ebb and flow research work, the evaluation of trust qualities for sensor hubs is for the most part in light of the correspondence (effective and unsuccessful interchanges) perspective. Truth be told, simply considering the correspondence conduct, we can't choose whether a sensor hub can be trusted or not. Other than the correspondence conduct, other trust measurements, for example, the vitality level ought to additionally be considered to compute the dependability of sensor hubs. Moreover, an effective trust model ought to manage instability brought about by uproarious correspondence channels and unsteady sensor hubs' practices.

2) There are two basic approaches to build up trust in WSNs: computing direct trust in view of direct associations and figuring backhanded trust esteem in light of suggestion from the outsider However, not all the third parties are trusty and not all the recommendations are reliable. Thus, a discriminate analysis about the third party and recommendation is essential.

3) Most existing concentrates just give the trust appraisal to neighbour hubs. Be that as it may, in genuine applications, a sensor hub some of the time needs to get the trust estimation of the non-neighbour hubs. For instance, in some directing conventions or limitation calculations sensor hubs require the data of the two-bounce neighbour hubs to set up the steering or restrict themselves. Along these lines, giving the trust evaluation to non-neighbour hubs turns out to be imperative.

4) Because of the dynamic topology, the trust relationship between sensor hubs always shows signs of change in WSNs. Trust are a dynamic marvel and changes with time and environment conditions. Be that as it may, most existing trust models don't tackle the trust dynamic issue. The advancement of trust after some time is another issue that needs advance study.

Keeping in mind the end goal to take care of the aforementioned issues, we propose a Efficient Distributed trust model (EDTM). The proposed EDTM can assess the trust connections between sensor hubs all the more exactly and can avoid security ruptures all the more successfully.

1.1 EDTM Structure

In this area, we portray the general design of EDTM. When we say hub B is dependable or dishonest for hub A, there is a trust model between hub A and hub B. As appeared in Fig. 1, EDTM comprises of four segments: direct trust, recommendation trust, indirect trust and update trust value When a subject node wants to obtain the trust value of an object, it first checks its recorded list of neighbour nodes. If the ID of the object node is in the list of neighbour nodes, the direct and recommendation trust model is triggered. Otherwise, the indirect trust model is started. If the trust is calculated based on node B’s direct experiences with node A completely, this model is called direct trust model. Otherwise, the recommendation trust model is built. Once the subject node A receives recommendations from other nodes about the object node B, indirect trust model can be established.

In current trust models, the direct trust and recommendation are always used to evaluate the trustworthiness of sensor nodes. The direct trust is directly calculated based on the communication behaviours between two

neighbour nodes. However, due to malicious attacks, using only direct trust to evaluate sensor nodes is not accurate. Thus, the recommendation from other sensor nodes is need to improve the trust evaluation. In addition, if the number of communication packets between two neighbour nodes is too small, it is difficult to decide whether an object node is good or bad based on only few interactions. We define a threshold of communication packets Th_{num}. If the communication packets between the subject and object nodes higher than the threshold Th_{num}, only the direct trust is calculated. Otherwise, the recommendation from the recommenders is needed for the object's trust evaluation.

The subject node first needs to select a set of recommenders. Then, the indirect trust is calculated based on recommendations and trust propagation. Next, we describe the detail calculation of direct, recommendation and indirect trust.

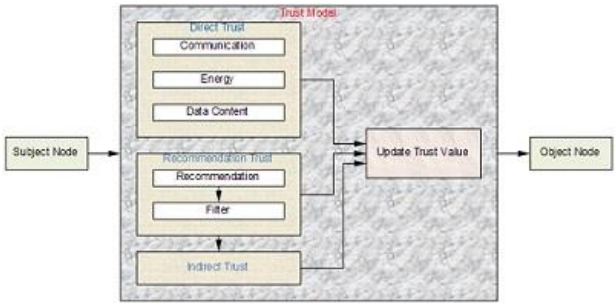

Fig. 1 EDTM Structure

2. Trust Calculation Using EDTM

The trust calculation is done using direct trust, indirect trust, and recommendation trust.

2.1. Direct Trust

The direct trust by considering communication trust, energy trust and data trust. The direct trust is calculated by the given eq. (1). The sensor nodes in WSNs usually collaborate and communicate with neighbour nodes to perform their tasks. Therefore, the communication behaviours are always checked to evaluate whether the sensor node is normal or not. However, due to the nature of wireless communication, there are many reasons resulting in the packets loss and the communications between sensor nodes are unstable. The unsuccessful communication maybe caused by malicious nodes or unstable communication channel. Therefore, just evaluating the communication behaviours is not enough for trust evaluation. In addition, communication trust, energy trust and data trust are defined in EDTM. The communication trust reflects if a sensor node can cooperatively execute the intended protocol. The energy trust is used to measure if a sensor node is competent in performing its intended functions or not. The data trust is the trust assessment of the fault tolerance and consistency of data, which affects the trust of the sensor nodes that create and manipulate the data. As shown in Fig.2

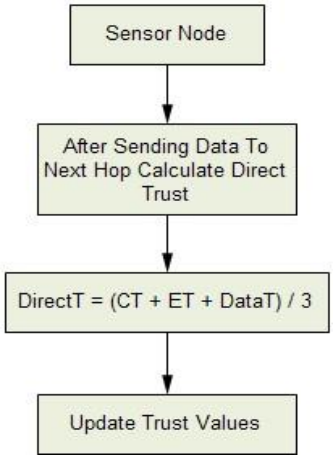

Fig. 2 Direct Trust

Direct Trust = (commtrust + datatrust + energytrust)/3 (1)

Calculation of the Communication Trust

The communication trust is based on Successful & Unsuccessful communication packets given in the eq. 2

commTrust = (2b+u)/2 (2)

Where b=success count / (Success count + Fail count + 1)

U=1 / (Success count + Fail count + 1)

Calculation of the Energy Trust

The energy trust is calculated using (Previous energy level – current energy level) (the energy consumption rate of normal nodes can maintain a stable value.)

If node energy level < Min requirement means => energy

Trust = 0 Otherwise calculate as bellow

1^{St} time energy > 2^{nd} time energy > …. >current time energy means => energy trust=1 otherwise this is malicious

Calculate Data Trust

The data trust is based on sensor node's data type. Same type of data or different type of data forward .The original node means same type of data only forward. Same type data means trust=1 otherwise 0.

2.2. Indirect trust

WSNs are multi-hop networks, when there are no direct communications between subject and object nodes, indirect trust can be established since trust is transitive. In this paper, the calculation of indirect trust includes two steps: 1) the first step is to find multi-hop recommenders between subject and object nodes, and 2) the second step is the trust propagation which aims at computing the direct trust. The path from the subject node to the object node

established by the recommenders is named as Trust Chain. As shown in Fig.3

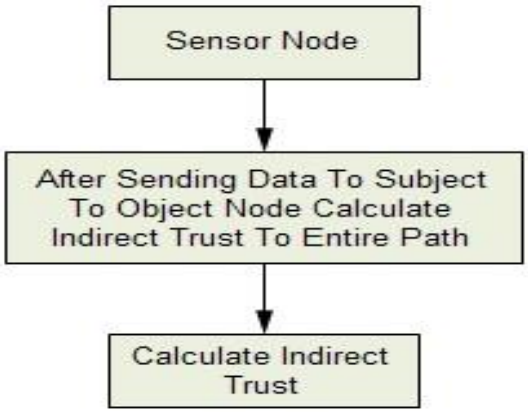

Fig. 3 Indirect Trust

2.3. Recommendation Trust

The recommendation trust is a special type of direct trust. As shown in the Fig. 4. When there are no direct communication behaviours between subject and object nodes, the recommendations from recommender are always taken into account for trust calculation .Based on the recommendations, the subject node filters the false recommendation using Recommendation Reliability and Recommendation Familiarity and computes the recommendation trust of object node using the eq.(3)

RT about Nth node =(0.5 + (Nth Node recommendation Value – 0.5) * T rel * T fam) / n (no of recommender) (3)

Recommendation Reliability

The Recommendation Reliability is calculated using the given eq. (4)

Trel = 1 – [particular neighbour given trust – all neighbour given trust average] (4)

Recommendation Familiarity

The Recommendation Familiarity is calculated using the given eq. (5)

Tfam = (Object & Recommender successful communication time/ Subject & recommender successful communication time) (5)

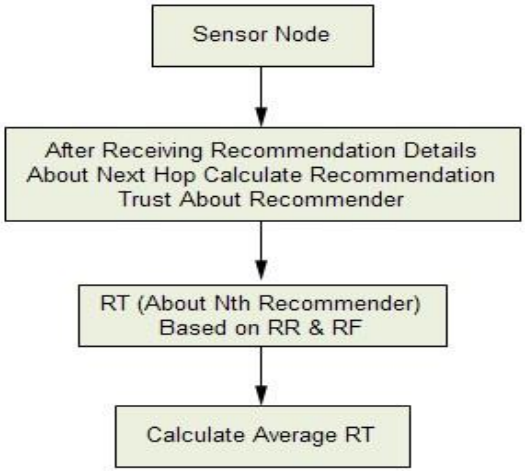

Fig. 4 Recommendation Trust

2.4. Find Malicious Node

Each sensor node calculates trust value on each and every communication. If the process continuously made, one stage malicious nodes are avoid to act intermediates. Base station monitor and identify the malicious node easily. As shown in the Fig. 5

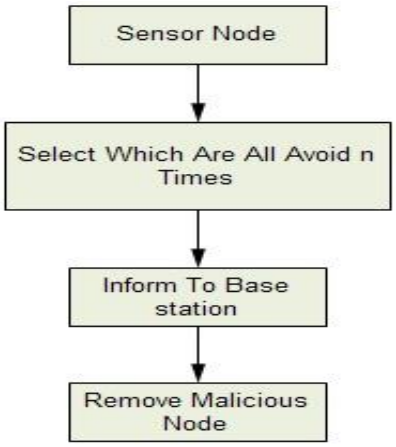

Fig. 5 Malicious Nodes

3. Simulation Results and Analysis

Our experiments are performed using NS2. First create network. Each sensor node send joining request to network server node after that send response (unique ID, Public & Private Key). Subject Sensor node Observer sense information and get end object sensor node name. After getting end object sensor name, send recommendation

request to all neighbour node. After receiving response from recommender node select forwarder node. Send information to intermediate / end object node. After sending the information calculates trust value for current transaction using EDTM and update new trust value to subject node. This process repeatedly made each transaction; one stage malicious nodes are automatically avoided for data forwarding.

3.1 Performance of EDTM

The trust value needs to be updated dynamically. It is generally known that frequent trust update wastes a lot of energy. On the contrary, if the trust update interval is too long, it cannot efficiently reflect the current behaviours of the object node. As shown in Fig. 6, the performance is calculated. At the beginning of the stimulation when the system is without malicious nodes, the trust value with longer update period grows slowly. Therefore, in order to save energy consumption, a longer update time period can be used for trust evaluation. However, the trust values calculated with malicious nodes under different time cycles are very different, thus shorter update time periods should be used.

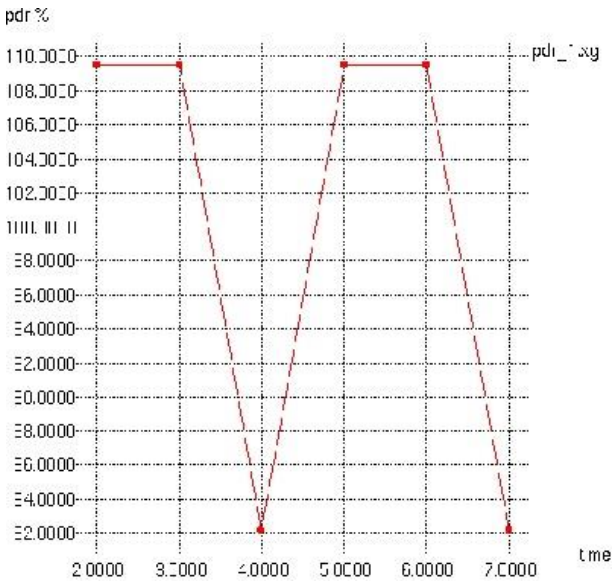

Fig. 6 Performance

4. Conclusion

The trust model has become important for malicious nodes detection in WSNs. It can assist in many applications such as secure routing, secure data aggregation, and trusted key exchange. Due to the wireless features of WSNs, it needs a distributed trust model without any central node, where neighbour nodes can monitor each

other. In addition, an efficient trust model is required to handle trust related information in a secure and reliable way. In this project, a distributed and efficient trust model named EDTM was proposed. During the EDTM, the calculation of direct trust, recommendation trust and indirect trust are discussed. Implementation results show that EDTM is an efficient and attack-resistant trust model.

Each sensor node calculates trust value on each and every communication. If the process continuously made, one stage malicious nodes are avoid to act intermediates. Base station monitor and identify the malicious node easily.

References

[1] Jinfang Jiang, Guangjie Han,Feng Wang and Lei Shu "An efficient distributed trust model for wireless sensor networks" IEEE Trans. On parallel and distributed systems, vol.26, no. 5, pp.1228-1237, May2015.

[2] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputationbased framework for high integrity sensor networks," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004, pp. 66–77.

[3] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst., 2008, pp. 437–446.

[4] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviours and d-s evidence theory," Sensors, vol. 11, pp. 1345–1360, 2011.

[5] G. Han, X. Xu, J. Jiang, L. Shu, and N. Chilamkurti, "The insights of localization through mobile anchor nodes in wireless sensor networks with irregular radio," KSII Trans. Internet Inf. Syst., vol. 6, pp. 2992–3007, 2012.

[6] H. S. Lim, Y. S. Moon, and E. Bertino, "Provenance based trustworthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sens. Netw., 2010, pp. 2–7.

[7] K. Shao, F. Luo, N. Mei, and Z. Liu, "Normal distribution based dynamical recommendation trust model," J. Softw., vol. 23, no. 12, pp. 3130–3148, 2012.

[8] K. Nordheimer, T. Schulze, and D. Veit, "Trustworthiness in networks: A simulation approach for approximating local trust and distrust values," IEEE Commun. Surveys Tuts., vol. 321, pp. 157–171, 2010.

[9] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 279–298, 2nd Quarter 2012.

[10] V. C. Gungor, L. Bin, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[11] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Managements and applications of trust in wireless sensor networks: A Survey," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.