International Journal of Research Instinct
(Peer-reviewed Journal)

ISSN ONLINE 2348-2095
Research Article

An Efficient Distributed Trust Model for Wireless Sensor Networks

[1]. J. Shabana, Dr . [2]. P. Srivaramangai,

[1].M.Phil – Research Scholar,[2].Asst Professor - Department of Computer Science

Srimad Andavan Arts and Science College (Autonomous),Trichy-5

srivara.padma@gmail.com

ABSTRACT

Nowadays trust models are one of the most important aspect to build up trust relationships among sensor nodes. Most of the existing works is missing the following problem. First problem is in the current research work, the assessment of trust values for sensor nodes is mainly based on the communication (successful and unsuccessful communications) point of View. Proposed work also considers other trust metrics such as the energy level should also be taken into account to calculate the trustworthiness of sensor nodes. Second there are two common ways to establish trust in WSNs: calculating direct trust based on direct interactions and calculating indirect trust value based on recommendation from the third party. 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. Third Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain trust value of the non-neighbor nodes. Therefore, providing the trust assessment on-neighbor nodes becomes very important. Fourth, because of the dynamic topology, the trust relationship between sensor nodes constantly changes in WSNs. Trust is a dynamic phenomenon and changes with time and environment conditions. However, most existing trust models do not solve the trust dynamic problem. In order to solve the above-mentioned problems, propose an **Efficient Distributed Trust Model** (EDTM) for WSNs. Implementation results will show that EDTM

outperforms other similar models, e.g., (**Node Behavioral strategies Banding belief theory of the Trust Evaluation**) NBBTE trust model.

Keywords: WSNs, EDTM, NBBTE

INTRODUCTION

NETWORK SECURITY DOMAIN INTRODUCTION

Computer security is a generic name for the collection of tools designed to protect data and to thwart hackers. Network security measures to protect data during their transmission. Internet security measures to protect data during their transmission over a collection of interconnected networks. Security attack is any action that compromises the security of information owned by an organization. Security mechanism is a process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Security service is a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability. Attack is an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

SCOPE OF THE PROJECT

In wireless sensor networks various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the

trustworthiness of another node. It is solved in our proposed model **Efficient Distributed Trust Model** (EDTM).

LITERATURE SURVEY

In Reputation-based Framework for High Integrity Sensor Networks author S. Ganeriwal, L. K. Balzano, and M. B. Srivastava[1] says the traditional approach of providing network security has beento borrow tools from cryptography and authentication. However,we argue that the conventional view of security based oncryptography alone is not sufficient for the unique characteristicsand novel misbehaviors encountered in sensor networks.Fundamental to this is the observation that cryptography cannotprevent malicious or non-malicious insertion of data from internaladversaries or faulty nodes using techniques Reputation-based Framework for Sensor Networks (RFSN)

In Parameterized and Localized trust management Scheme for sensor networks security authors Z. Yao, D. Kim, and Y. Doh[2] says the wireless and resource-constraint natureof a sensor network makes it an ideal medium for attackersto do any kinds of vicious things. In this paper, we describe*PLUS*, a parameterized and localized trust managementscheme for sensor networks security, where each sensornode maintains highly abstracted parameters, rates thetrustworthiness of its interested neighbors to adopt appropriatecryptographic methods, identify the maliciousnodes, and share the opinion locally.

In Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory authors R. Feng, X. Xu, X. Zhou, and J. Wan[3] says wireless sensor networks (WSNs), many factors, such as mutual interference of wireless links, battlefield applications and nodes exposed to the environment without good physical protection, result in the sensor nodes being more vulnerable to be attacked and compromised. In order to address this network security problem, a novel trust evaluation algorithm defined as NBBTE (Node Behavioral Strategies Banding Belief Theory of the Trust Evaluation Algorithm) is proposed, which integrates the approach of nodes behavioral strategies and modified evidence theory. According to the behaviors of sensor nodes, a variety of trust factors and coefficients related to the network application are established to obtain direct and indirect trust values through

calculating weighted average of trust factors. Meanwhile, the fuzzy set method is applied to form the basic input vector of evidence. On this basis, the evidence difference is calculated between the indirect and direct trust values, which link the revised D-S evidence combination rule to finally synthesize integrated trust value of nodes.

In The Insights of Localization through Mobile Anchor Nodes in Wireless Sensor Networks with Irregular Radio authors G. Han, X. Xu, J. Jiang, L. Shu, and N. Chilamkurti[4] says, Recently there has been an increasing interest in exploring the radio irregularity research problem in Wireless Sensor Networks (WSNs). Measurements on real test-beds provide insights and fundamental information for a radio irregularity model. In our previous work "LMAT", we solved the path planning problem of the mobile anchor node without taking into account the radio irregularity model. This paper further studies how the localization performance is affected by radio irregularity. There is high probability that unknown nodes cannot receive sufficient location messages under the radio irregularity model. Therefore, we dynamically adjust the anchor node's radio range to guarantee that all the unknown nodes can receive sufficient localization information. In order to improve localization accuracy, we propose a new 2-hop localization scheme. Furthermore, we point out the relationship between degree of irregularity (DOI) and communication distance, and the impact of radio irregularity on message receiving probability.

EXISTING SYSTEM

Various existing approaches are still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes.Existing distributed Reputation-based Framework for Sensor Networks (RFSN) is two key building blocks (Watchdog and Reputation System). Watchdog is responsible for monitoring communication behaviors of neighbor nodes. Reputation System is responsible for maintaining the reputation of a sensor node. The trust value is calculated based on the reputation value. It is calculated only the direct trust while the recommendation trust is ignored.

PROPOSED SYSTEM

Proposed systems during the trust calculation not only consider the communication behavior, also consider other trust metrics such as the energy level should also be taken into account to calculate the trustworthiness of sensor nodes. In addition, an efficient trust model should deal with uncertainty caused by noisy communication channels and unstable sensor nodes' behaviorsbecause of the dynamic topology, the trust relationship between sensor nodes constantly changes in WSNs. Trust is a dynamic phenomenon and changes with time and environment conditions. However, most existing trust models do not solve the trust dynamic problem. In order to solve the above-mentioned problems, we propose an efficient distributed trust model (EDTM). The proposed EDTM can evaluate the trust relationships between sensor nodes more precisely and can prevent security breaches more effectively.

ALGORITHM

Trust Calculation in EDTM

1) **The Calculation of Direct Trust**

- ✓ **Calculation of the Communication Trust** – Based on Successful & Unsuccessful communication packets

  commTrust = (2b+u)/2

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

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

- ✓ **Calculation of the Energy Trust** – (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** – Based on sensor node's data type. Same type of data or different type of data forward (If original node means same type of data only forward)

  Same type data means trust=1 otherwise 0.

Direct trust = (Comtrust + energytrust + datatrust) / 3

Recommendation Trust Calculation (Receive RecommendationT & (SuccessCount on recommender & object))

Recommendation Reliability

Reli Trust = 1 – [particular neighbor given trust – all neighbor given trust average]

Recommendation Familiarity

Trust fami = (Object & Recommender successful communication time/ Subject & recommender successful communication time)

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

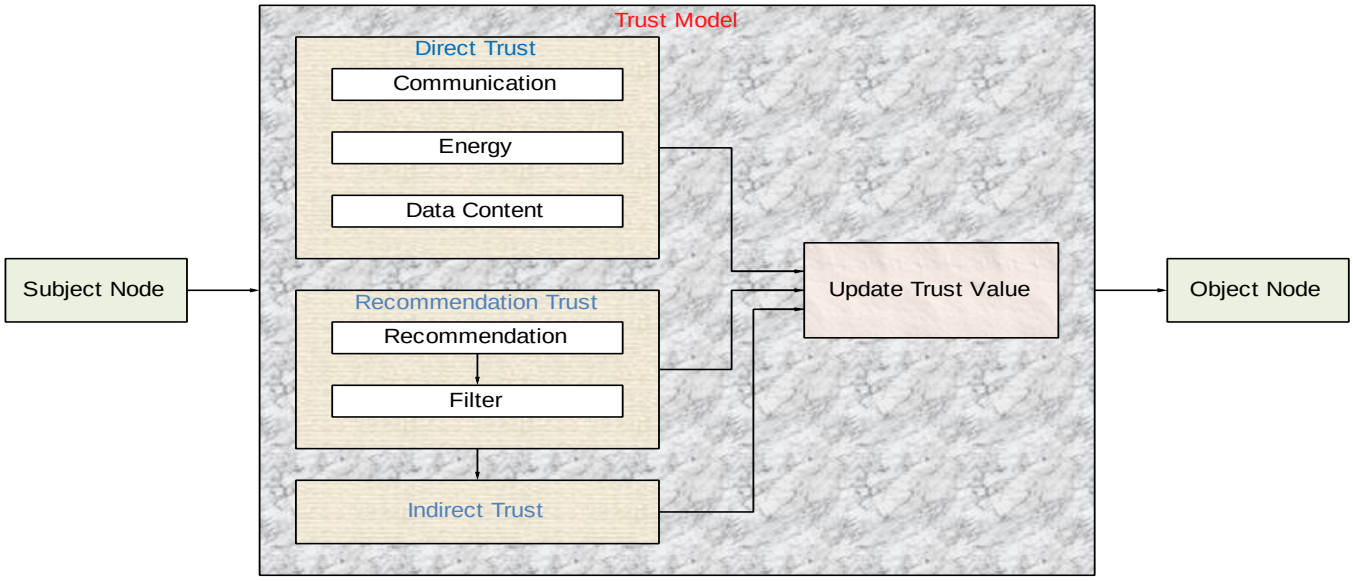
2) Calculation of the Indirect Trust

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

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.

Architecture



CONCLUSION

The trust model has become important for malicious node 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 neighbor 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.

REFERENCES

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

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

[3]. R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithmfor wireless sensor networks based on node behaviors and d-s evidencetheory," Sensors, vol. 11, pp. 1345–1360, 2011.

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

[5]. H. S. Lim, Y. S. Moon, and E. Bertino, "Provenance based trustworthinessassessment in sensor networks," in Proc. 7th Int. WorkshopData Manage. Sens. Netw., 2010, pp. 2–7.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.