International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 7 (July '2016)

AN EFFICIENT DISTRIBUTED TRUST MODEL FOR WIRELESS SENSOR NETWORKS

J. Shabana,
Research Scholar,
Department of Computer Science,
Srimad Andavan Arts & Science College (Autonomous)
India.

Dr. P. Srivaramangai,
Assistant Professor,
Department of Computer Science,
Srimad Andavan Arts & Science College (Autonomous)
India.

Abstract: Nowadays trust models are one of the most important to build up trust relationships among sensor nodes. Most of the existing work 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 the trust value of the non-neighbor nodes. Therefore, providing the trust assessment for non-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: Trust Model, Wireless Sensor Network, Efficient Distributed Trust Model

I.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.

Trust models have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). Considerable research has been done on modeling trust. However, most current research work only takes communication behavior into account to calculate sensor nodes' trust value, which is not enough for trust evaluation due to the widespread malicious attacks.

- 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. In fact, just considering the communication behavior, we cannot decide whether a sensor node can be trusted or not. Besides the communication behavior, 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' behaviors.
- 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.
- Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. For example, in some routing protocols or localization algorithms sensor nodes need the information of the two-hop neighbor nodes to establish the routing or localize themselves. Therefore, providing the trust assessment for non-neighbor nodes becomes very important.
- 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. The evolution of trust over time is another problem that needs further study. 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.

II.PROBLEM DEFINITION

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).

III. LITERATURE SURVEY

- **Title: Reputation-based Framework for High Integrity Sensor Networks**
  Author: S. Ganeriwal, L. K. Balzano, and M. B. Srivastava

INTRODUCTION

The traditional approach of providing network security has been to borrow tools from cryptography and authentication. However, we argue that the conventional view of security based on cryptography alone is not sufficient for the unique characteristics and novel misbehaviors encountered in sensor networks. Fundamental to this is the observation that cryptography cannot prevent malicious or non-malicious insertion of data from internal adversaries or faulty nodes.

We believe that in general tools from different domains such as economics, statistics and data analysis will have to be combined with cryptography for the development of trustworthy sensor networks. Following this approach, we propose a reputation-based framework for sensor networks where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. We will show that this framework provides a scalable, diverse and a generalized approach for countering all types of misbehavior resulting from malicious and faulty nodes.

USED TECHNIQUE

- ✓ Reputation-based Framework for Sensor Networks (RFSN)

(A distributed Reputation-based Framework for Sensor Networks (RFSN) is first proposed for WSNs. Two key building blocks of RFSN are 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. However, in RFSN, only the direct trust is calculated while the recommendation trust is ignored.)

DRAWBACK

- Calculated only the direct trust while the recommendation trust is ignored.
- **Title: PLUS: Parameterized and Localized trust management Scheme for sensor networks security**
  Author: Z. Yao, D. Kim, and Y. Doh

INTRODUCTION

The wireless and resource-constraint nature of a sensor network makes it an ideal medium for attackers to do any kinds of vicious things. In this paper, we describe *PLUS*, a parameterized and localized trust management scheme for sensor networks security, where each sensor node maintains highly abstracted parameters, rates the trustworthiness of its interested neighbors to adopt appropriate cryptographic methods, identify the malicious nodes, and share the opinion locally.

USED TECHNIQUE

- ✓ Parameterized and Localized trUst management Scheme (PLUS)

(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 behaviors or not. Therefore, suspect node may get unfair penalty.**)**

DRAWBACK

- It always checks 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 behaviors or not. Therefore, suspect node may get unfair penalty.
- **Title: A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory**
  Author: R. Feng, X. Xu, X. Zhou, and J. Wan

INTRODUCTION

For 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.

USED TECHNIQUE

- ✓ Node Behavioral strategies Banding belief theory of the Trust Evaluation (NBBTE)

(NBBTE algorithm first establishes various trust factors depending on the communication behaviors between two neighbor nodes. Then, it applies the fuzzy set theory to measure the direct trust values of sensor nodes. Finally, considering the recommendation of neighbor 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 behaviors to evaluate the trustworthiness of sensor nodes.)

DRAWBACK

- NBBTE only takes the selective forwarding attack so, with the increase number of malicious nodes, the detection rate decreases rapidly.
- In NBBTE, each node needs to store the information for all the sensor nodes in the network so nodes occupy more memory space.
- **Title: The Insights of Localization through Mobile Anchor Nodes in Wireless Sensor Networks with Irregular Radio**

Author: G. Han, X. Xu, J. Jiang, L. Shu, and N. Chilamkurti

INTRODUCTION

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.

USED TECHNIQUE

- ✓ Localization algorithm with a Mobile Anchor based on Triangulation in WSNs (LMAT)

(Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. In some routing protocols sensor nodes need the information of the two-hop neighbor nodes to establish the routing or localize themselves. Therefore, providing the trust assessment for non-neighbor nodes becomes very important so in this paper consider trust assessment for non-neighbor nodes)

DRAWBACK

- Sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. Mainly focus that only.
- **Title: Provenance based Trustworthiness Assessment in Sensor Networks**

Author: H. S. Lim, Y. S. Moon, and E. Bertino

INTRODUCTION

As sensor networks are being increasingly deployed in decision-making infrastructures such as battlefield monitoring systems and SCADA (Supervisory Control and Data Acquisition) systems, making decision makers aware of the trustworthiness of the collected data is a crucial. To address this problem, we propose a systematic method for assessing the trustworthiness of data items. Our approach uses the data provenance as well as their values in computing trust scores, that is, quantitative measures of trustworthiness. To obtain trust scores, we propose a cyclic framework which well reflects the inter-dependency property: the trust score of the data affects the trust score of the network nodes that created and manipulated the data, and vice-versa. The trust scores of data items are computed from their value similarity and provenance similarity. The value similarity comes from the principle that "the more similar values for the same event, the higher the trust scores". The provenance similarity is based on the principle that "the more different data provenances with similar values, the higher the trust scores".

USED TECHNIQUE

- ✓ Value similarity
- ✓ Provenance similarity

(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 are. We thus propose a systematic approach for computing trust scores based on value similarity under the distribution of collected data. Provenance similarity is based on the observation that different provenances of similar data values may increase the trustworthiness of data items.)

DRAWBACK

- Trust value based on only Value similarity, Provenance similarity and energy level for previous and current.

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.
- A Parameterized and Localized trUst management Scheme (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 behaviors or not. Therefore, suspect node may get unfair penalty.

DRAWBACK

- ✓ Indirect trust calculation method in NBBTE cannot reasonably reflect the sensor nodes' real trust level.
- ✓ NBBTE only takes the selective forwarding attack so, with the increase number of malicious nodes, the detection rate decreases rapidly.
- ✓ Both EDTM and NBBTE are robust against the data forgery attack, but EDTM works better.
- ✓ In NBBTE, each node needs to store the information for all the sensor nodes in the network so nodes occupy more memory space.

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' behaviors.
- There are two common ways to establish trust in WSNs: calculating direct trust based on direct interactions and

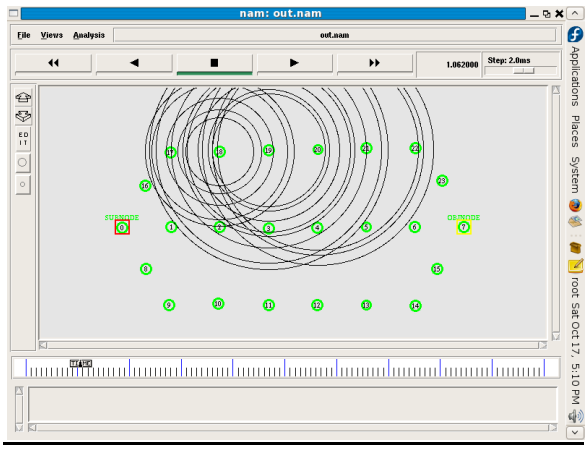
calculating indirect trust value based on recommendation from the third party. However, not all the third parties are trusty and not all the recommendations are reliable. Thus, a discriminate analysis about the third party and recommendation is essential. Our proposed systems have recommendation trust.

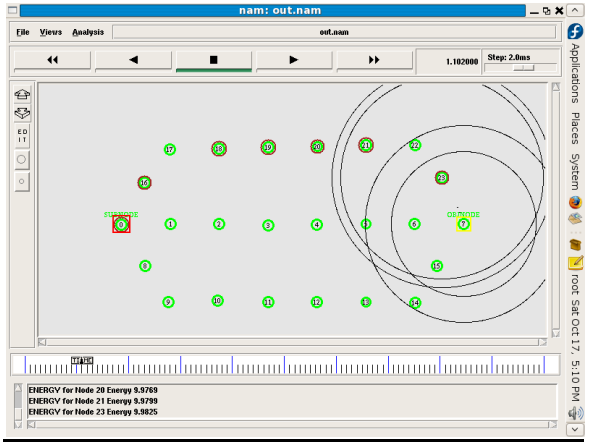
- Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. Sensor nodes need the information of the two-hop neighbor nodes to establish the routing or localize themselves. Therefore, providing the trust assessment for non-neighbor nodes becomes very important. Our proposed systems have indirect trust value. It is gained based on the recommendations from other nodes.
- 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, 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.

ADVANTAGE

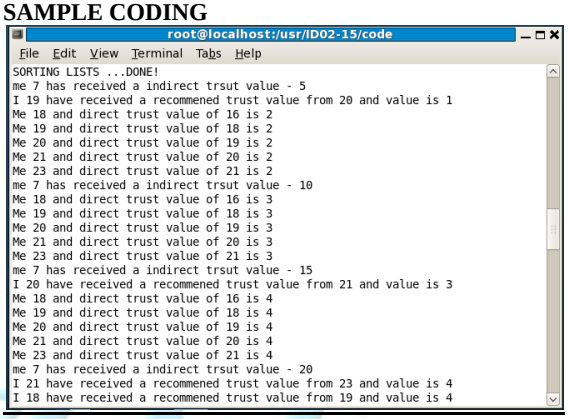
- ✓ Secure communications and ensure that all communicating nodes are trusted.
- ✓ EDTM outperforms NBBTE in terms of indirect trust value calculation.
- ✓ In EDTM increase the number of malicious nodes, the detection rate is robust to the five kinds of malicious attacks.
- ✓ In data forgery attack EDTM perform better than to NBBTE.
- ✓ EDTM is much more energy efficient, because in EDTM sensor nodes interact only with their neighbor nodes. As a result, nodes do not keep trust information about every node in the network. Only keeping neighborhood information implies significant lower energy consumption, less processing for trust level calculation, and less memory space.

SCREEN SHOTS





SAMPLE CODING



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 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.

FEATURE ENHANCEMENT

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.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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, pp. 1345–1360, 2011.

[4]. 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.

[5]. 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.

[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.

