International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 26 Issue 7 – DECEMBER 2019.

EFFECTIVE DISTRIBUTED TRUST MODEL (EDTM) MORE EFFICIENT FOR WIRELESS SENSOR NETWORKS

V.Elakiya [#1],A.Banupriya[*2],J.Kalpana [*3]

[#] *Assistant Professor, Dept of CSE, CK College of Engineering and Technology, Cuddalore, Tamilnadu, India*

[*] *Student, Dept of CSE, CK College of Engineering and Technology, Cuddalore, Tamilnadu, 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 Bandingbelief theory of the Trust Evaluation) NBBTE trust model.**

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

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.A variety of attacks available in wireless sensor networks a classification of the attacks consists in distinguishing the passive attacks from the active attacks.

The passive attack (eavesdropping) is limited to listening and analyzes exchanged traffic. This type of attacks is easier to realize (it is enough to have the adequate receiver), and it is difficult to detect. Since, the attacker does not make any modification on exchanged information. The intention of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network (cluster head node), by analyzing routing information, to prepare an active attack.In the active attacks, an attacker tries to remove or modify the messages transmitted on the network. He can also inject his own traffic or replay of old messages to disturb the operation of the network or to cause a denial of service. Among the most known active attacks, we can quote:

Tampering: it is the result of physical access to the node by an attacker; the purpose will be to recover cryptographic material like the keys used for ciphering.

Black hole: a node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network.

Selective forwarding: as mentioned above, a node play the role of router, in a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them.

Sybil attack: "malevolent device, taking multiple identities in an illegitimate way", attacker can use the identities of the others nodes in order to take part in distributed algorithms such as the election.

HELLO flood attack: many routing protocols use "HELLO" packet to discover neighboring nodes and thus to establish a topology of the network. The simplest attack for an attacker consists in sending a flood of such messages to flood the network and to prevent other messages from being exchanged.

Jamming: a well-known attack on wireless communication, it consists in disturbing the radio channel by sending useless information on the frequency band used. This jamming can be temporary, intermittent or permanent.

Blackmail attack: a malicious node makes announce that another legitimate node is malicious to eliminate this last from the network. If the malicious node manages to tackle a significant number of nodes, it will be able to disturb the operation of the network.

Exhaustion: is to consume all the resources energy of the victim node, by obliging it to do calculations or to receive or transmit unnecessarily data.

Wormhole attack: attackers here are strategically placed at different ends of a network. They can receive messages and replays them in different parts by means of a tunnel.

Identity replication attack: attacker can clone nodes, and place it in different part of the network in order to collect majority of information traffic. Unlike the Sybil attack, the identity replication attack is based upon giving the same identity to different physical nods. This attack can be mounted because in a WSN there is no way to know that a wireless sensor node is compromised.

II. PROBLEM DEFINITIONS

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. RELATED WORKS

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.

IV. DRAWBACKS

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.

V. METHODOLOGY

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.

VI. ADVANTAGES

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.

VII. ALGORITHM USED

A. *EDTM*

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

1St time energy > 2nd 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

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)

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:

The first step is to find multi-hop recommenders between subject and object nodes

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.

VIII. SYSTEM ARCHICHTURE

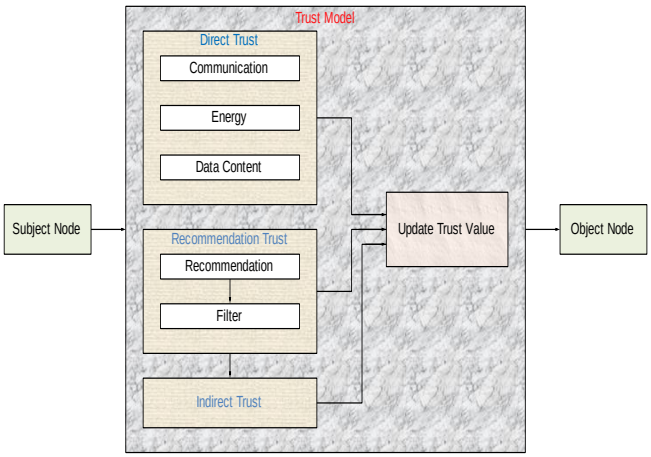

Figure 1 System Architecture

IX. 10 RESULT

Creating a 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 neighbor 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.

X. CONCLUSION

The trust model has become important for malicious nodes detection in WSNs. It can assist in many 6 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.

XI. FUTURE ENHANCEMENT

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