RESEARCH ARTICLE OPEN ACCESS

Secure Transmission of Information in Wireless Sensor Networks Using EDTM

V.Mahalakshmi[1], M.Meenakshi[2],G.Megala[3], Ms.B.Revathi M.E.[4]
[1,2,3](ECE, S.A.Engineering College, Thiruverkandu, Chennai, INDIA)

Abstract:

For the secure transfer of information in wireless sensor networks, trust model have been recommended as an effective security mechanism. Many factors such as wireless links mutual interference and nodes exposed to the environment without physical protection makes the sensor nodes to be attacked. In current researches only the communication behavior of the sensor nodes are used to calculate the trust value which is not enough due to malicious attacks. In this paper we propose an Efficient Distributed Trust Model (EDTM). Based on the number of packets transferred between the sensor nodes direct and recommendation trust are calculated. The trustworthiness of sensor node is evaluated accurately by using the proposed EDTM and it prevents the security breaches more significantly. The experimental result shows that the EDTM can outperform other similar model.

Keywords — **security in wireless sensor networks, management of trust, energy efficient.**

I. INTRODUCTION

WSN is a one of the type of ad-hoc network. WSN is a collection of tiny disposable and two power devices. Wireless sensor networks enable reliable monitoring and analysis of unknown and untested environments. Sensor devices sensing module, a communication module, memory and an exhaustible source of power like a small battery. WSN are used in many applications such as emergency response [1], monitoring of health [2], power grid and traffic management [3] etc.

To avoid the security threats, various security mechanisms are proposed such as Cryptography, Authentication and Message integrity, etc. However, they suffer from many vulnerabilities. The external attacks only can be solved by traditional security mechanisms. To establish secure communication, we need to ensure that all communicating nodes are trusted. To build the trust relationship among the sensor nodes [4] trust models have developed by the researchers.

II. SYSTEM OUTLINE

The previously designed system takes the following barriers:

In the current systems, the trust values are based on the communication behaviour. The trust dynamic problem cannot be solved. Providing trust assessment for non-neighbor nodes becomes very important (e.g.) TPGFPlus [8] and improved LMAT Algorithm [9]. Updating of trust value can take more time and the Trust over time is another problem. The true and false recommendations are not distinguished.

Reputation based Frame work for Sensor Networks (RFSN) [5] was the first proposed for WSN. Reputation system and Watchdog are the two blocks of RFSN. The reputation of a sensor node can be maintained by the reputation system. Watchdog is used for monitoring the communication behaviors of the neighboring nodes. Only direct trust is calculated using RFSN.

Later Parameterized and Localized trUst management Scheme (PLUS) [6] was proposed. Whenever a judge node receives packets from suspect node it checks for integrity. If the integrity fails, trust of suspect node will be decreased and it gets unfair penalty.

Another similar algorithm named Node Behavioral Strategies Banding belief theory of the

Trust Evaluation algorithm (NBBTE) was proposed based on behavior strategy banding D-S belief theory [7]. It establishes various trust factors to evaluate the trustworthiness of sensor nodes.

A. *System Design*

There are three nodes namely subject node, recommender and object node. Node A is named as subject node and node B is the object node. It is multiport network i.e the sensor nodes directly communicate with the neighbor nodes within their communication range.

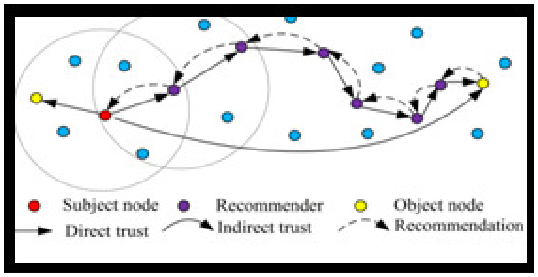


Fig.1.Netwrok architecture

III. STRUCTURE OF EDTM

EDTM consists of two main components: One-hop trust model and Multi-hop trust model which includes following six components: direct trust module, recommendation trust module, indirect trust module, integrated trust module and trust propagation module.

When subject node wants to obtain trust values of an object, it checks the recorded list of neighbor nodes. If the id of the object node is in the list of the neighbor node, one-hop trust model is triggered or multi-hop trust model is started. In one-hop trust model, if the trust is calculated based on direct experience of the two nodes, it is called as direct trust module. Otherwise, the recommendation trust module is build. In the multi-hop trust model, if the subject node A receives recommendation from other nodes about B, indirect trust module is established.

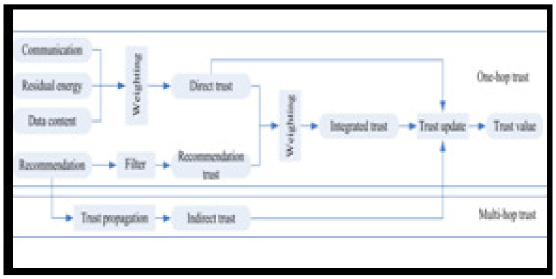


Fig.2.Structure of EDTM

IV. TRUST CALCUATION IN EDTM

In the literature [10], many definitions given to the trust. Trust is always defined by reliability, utility, availability, risk, quality of service. Trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors. That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs. In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite.

Trust has three important properties [11] and [12]. They are asymmetry, transitivity and Composability. Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A. Transitivity means the trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. The transitivity is a very important property in trust calculation between two non-neighbor nodes. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

A.Calculation of Direct Trust

Direct trust is composed by considering communication trust, energy trust and data trust. The sensor nodes in WSN usually collaborate and communicate with neighbor nodes to evaluate whether the sensor node is normal or not.

B.Communication Trust

The communication trust reflects if a sensor node can cooperatively execute the intended protocol. It is also based on sensor nodes prior communication behavior. If the communication channel between two sensor nodes are unstable and noisy, monitoring the previous communication behavior becomes uncertainty. So we adopt a subjective logic framework [13] which is a triplet T = {b, d, u} where b, d, u corresponds to belief, disbelief and uncertainty. The communication trust is calculated based on successful (s) and unsuccessful (f) communication packets.

$$T_{com} = \frac{2b+u}{2} \qquad (1)$$

Where,

$$b = \frac{s}{s+f+1}, \; u = \frac{1}{s+f+1}$$

C.Calculation of Energy Trust

The energy trust is used to measure if the sensor node is competent in performing its intended function or not. An energy threshold θ is defined. When residual energy E_{res} falls below the threshold value then the energy trust is considered to be 0. Otherwise the trust is calculated based on energy consumption rate as follows

$$\text{Tene} = \begin{cases} 1 - \text{pene}, & Eres \geq \Theta \\ 0, & else \end{cases} \qquad (2)$$

Where pene is calculated based on ray projection method [15].

D.Calculation of data trust

The data trust is the trust assessment of the fault tolerance and consistency of data, which affects the trust of sensor nods that create and manipulate the data. It is based on probability distribution function [17]. If the value of data items is close to mean the trust value is high and vice-versa. Therefore data trust is calculated by

$$T(data) = 2\int_{vd}^{\infty} f(x)dx \qquad (3)$$

E.Recommendation trust

The recommendation trust is a special type of direct trust. As shown in fig.3, When subject node wants to obtain recommendations of an object node B, it transmits the recommendation request message t the neighboring nodes. Upon receiving the request message, the qualified nodes will reply if they have recommendation of node B. Based on the recommendation node A filters the false recommendation and compute the recommendation trust of node B.

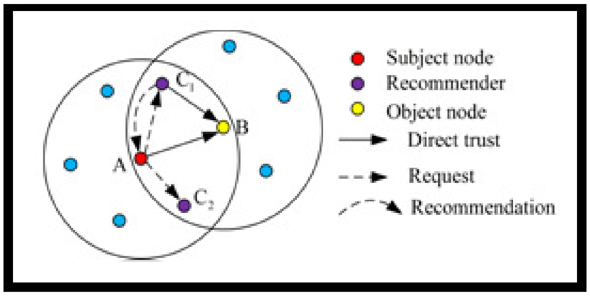


Fig 3.Recommendation trust

F.Indirect Trust

It includes three selection mechanisms. The first selection mechanism can find the shortest trust chain, thus communication overhead for indirect trust calculation can be minimized. The second selection mechanism can choose the must believable trust chain but it is not energy efficient. Third selection mechanism is the best one. The subject node A is broadcast a recommendation request message to its next hop recommender and waits for reply. Upon receiving a request message the recommender will check if they have any information needed by node A. If object node B is not a neighbor node of current recommender it continually forward the request message to its next hop recommenders.

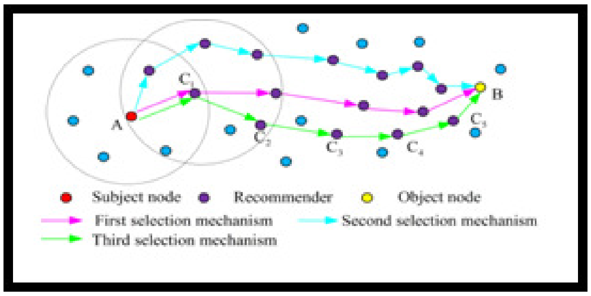

C1
A
C2
C3
C4
C5
B
Subject node
Recommender
Object node
First selection mechanism
Second selection mechanism
Third selection mechanism

Fig 4.Indirect Trust

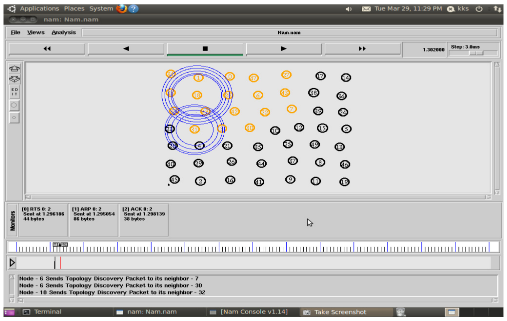
V. PERFORMANCE EVALUATION

A. Simulation Parameters

The network simulator ns-2 [11] has been implemented for the proposed scheme and its performance compared with some existing mechanisms. The 802.11 MAC layer implemented in ns-2 is used for simulation. The nodes which has the trust value less than 0.4 are taken as malicious, nodes with trust level between 0.4 and 0.9 are assumed be suspected and those with trust value greater than 0.9 are assumed to be trusted.

In every one-minute interval, the trust values are exchanged. Each node has a buffer capacity of 64 packets with secure routing protocol.The detection rate of malicious node and the energy consumption of EDTM and NBBTE are compared. The deployment area is set to be 100*100m. There are 100 sensor nodes deployed randomly in the sensing area. The nodes which are affected are simulated by the following five kinds of malicious attacks: selective forwarding attack, data forgery attack, DoS attack, on/off attack, bad and good mouthing attack. In order to compare the subjective trust value calculated by a sensor node, the objective trust is also derived.

Based on the actual information of each node without considering any network dynamics such as node mobility, trust decay over time and any malicious attacks the objective trust is calculated. Therefore, the subjective trust values are mostly lower than the objective trust values.



[0] RTS 0: 2
Sent at 1.296186
44 bytes

[1] ARP 0: 2
Sent at 1.295054
86 bytes

[2] ACK 0: 2
Sent at 1.298139
38 bytes

```
Node - 6 Sends Topology Discovery Packet to its neighbor - 7
Node - 6 Sends Topology Discovery Packet to its neighbor - 30
Node - 18 Sends Topology Discovery Packet to its neighbor - 32
```

Fig 5 network topology

Performance metrics: The performance of the proposed EDTM approach are evaluated by using the following metrics such as the residual energy, detection radio and trust values.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Packet Size	512 bytes
Channel data rate	11 Mbps
Area	100m*100m
Simulation time	800

VI. SIMULATION RESULTS

The proposed algorithm with results obtained in this simulation used the performance metrics to validate.

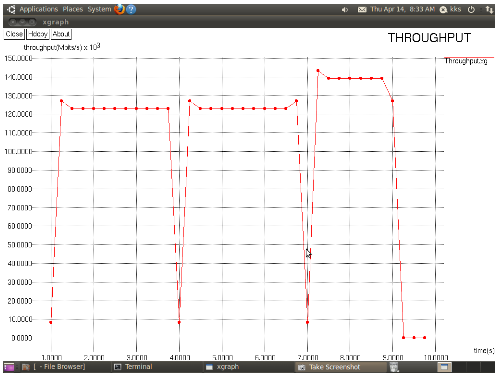


Fig 6 throuput

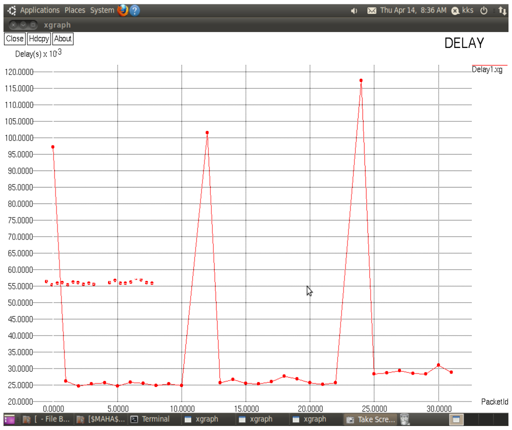


Fig 7 Delay

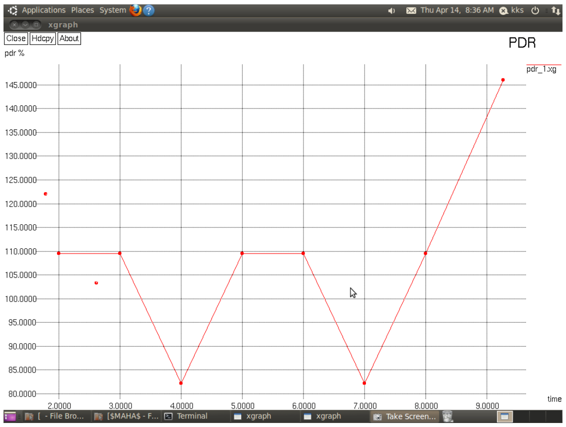


Fig 8 PDR

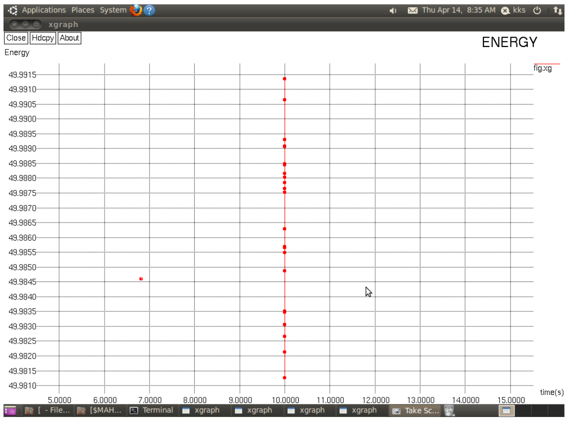


Fig 9 Energy

The existing system can be compared with the proposed ETDM and it shows that EDTM is very efficient and effective.

VII. CONCLUSION

The trust model has became very important for the detection of malicious nodes in the wireless sensor network. In many applications such as secure routing, secure data aggregation and trusted key exchange EDTM can assist. Because of the wireless and resource constraint features of WSNs, WSN needs a distributed trust model without any central node, where neighbor nodes can monitor each other. Trust model is required to handle trust related information in a secure and reliable way. In this paper, a efficient and distributed trust model named EDTM is proposed. The calculation of direct trust, recommendation trust and indirect trust are discussed in the EDTM. Trust propagation and update are studied in this paper. Simulation results show that EDTM is an efficient and attack-resistant trust model. In our future research, we plan to address the threshold definition and the selection of proper value of the weight which is still a challenge problem.

VIII. REFERENCES

[1] H. Chan and A.Perrig, "Security and Privacy in Sensor Networks".IEEE Computer, Vol. 36, No. 10, pp. 103-105, 2003.

[2] Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park, "Pervasive, Secure Access to a Hierarchical-based Healthcare Monitoring Architecture in Wireless Heterogeneous Sensor Networks". IEEE Journal on Selected Areas of Communications, Vol. 24, No. 7, pp. 400-411, May 2009.

[3] V.C. Gungor, L. Bin, and G.P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid". IEEE Transactions on Industrial Electronics, Vol. 57, No. 10, pp. 3557-3564, 2010.

[4] G. Han, J. Jiang, L. Shu, J. Niu and H.C. Chao, "Managements and applications of trust in Wireless Sensor Networks: A Survey". Journal of Computer and System Sciences, pp. 1-16, 2013.

[5] S. Ganeriwal, L.K. Balzano and M.B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks". In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 66-77, 2004.

[6] Z. Yao, D. Kim and Y. Doh, "PLUS: Parameterized and Localized trust management Scheme for sensor networks security". IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 437-446, 2008.

[7] 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, pp. 1345-1360, 2011.

[8] G. Han, Y. Dong, H. Guo, L. Shu, D. Wu, "Cross-layer Optimized Routing in WSN with Duty-cycle and Energy Harvesting". Wireless Communications and Mobile Computing, 2013 accepted.

[9] 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 Transactions on Internet and Information Systems, pp. 2992-3007, 2012.

[10] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey". IEEE communications survey and tutorials, Vol.14, No. 2, pp. 279-298, 2012.

[11] K. Nordheimer, T. Schulze, and D. Veit, "Trustworthiness in networks: A simulation approach for approximating local trust and tutorials, pp. 157-171, 2010.

[12] A. Josang, "An algebra for assessing trust in certification chains". In Proceedings of the Network and Distributed Systems Security Symposium, pp. 1-10, 1999.

[13] W. Gao, G. Zhang, W. Chen and Y. Li, "A Trust Model Based on Subjective Logic". the Fourth International Conference on Internet Computing for Science and Engineering, pp. 272-276, 2009.

[14] M. Chen, Y. Zhou and L, Tang, "Ray projection method and its applications based on Grey Prediction". the Chinese Journal of Statistics and Decision, Vol.1, pp. 13. 2007.

[15] H.S. Lim, Y.S. Moon and E. Bertino, "Provenance based Trustworthiness Assessment in Sensor Networks".In Proceedings of the 7th International Workshop on Data Management for Sensor Networks, pp. 2-7, 2010.

[16] E. Elnahrawy and B. Nath, "Cleaning and Querying Noisy Sensors". In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp. 78-87. 2003.

[17] K. Shao, F. Luo, N. Mei and Z. Liu, "Normal Distribution Based Dynamical Recommendation Trust Model". Journal of Software, Vol. 23, No. 12, pp. 3130-3148, 2012.