International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

AN EFFICIENT DISTRIBUTED TRUST MODEL FOR SECURE TRANSMISSION IN WIRELESS SENSOR NETWORK

S.Shashank [1], R. Precila[2]

[1]*UG student, Department of CSE, RMK Engineering College, Tiruvallur, Tamilnadu.*
[2]*Assistant Professor, Department of CSE, RMK Engineering College, Tiruvallur, Tamilnadu.*

***Abstract*- 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, an efficient distributed trust model is proposed. First, according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. Furthermore, trust reliability and familiarity are defined to improve the accuracy of recommendation trust. The trust analysis is performed here based on the honesty, reliability and the effective parameters. The proposed EDTM can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more significantly. The experimental results represents that proposed model outperforms other similar models, e.g., NBBTE trust model.**

Index Terms- Trust management, Security in wireless sensor networks, Auto trust and recommended trust.

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. There are some crucial aspects we always need to keep in mind when employed with these networks; security is one of them. We absolutely can't depend on any of our objects to be tamper-proof or use any kind of "trusted" computing platform since these characteristics often make the individual nodes prohibitively expensive. Security stipulation often vary with application and framework, but in general, security for wireless sensor networks should focus on the protection of the data itself and the network connections among the nodes. Some of the valuable data security requirements are confidentiality, integrity and authentication. When taking the network into consideration, we need to protect fair access to communications channels and we often need to obscure the physical location of our nodes. We must protect against malicious resource consumption, denial of service attacks, node capturing and node injection. Sometimes to guard the network from the effects of malicious nodes, secure routing is required by applications [1].

Because the communication among sensor nodes in a WSN is done by wireless transceivers, which tend to be extremely vulnerable to simple node attacks, shortcomings in a subsystem can easily be exploited to put on attacks on the whole network, even beyond the "sink." So it is very important to design sensor networks with security in mind from their design stage, not as an additional feature of the system. Its main reason is that security always add some overhead, such as increased power requirements—something that's difficult to introduce in to an already-designed system. Firm coalition of security mechanisms in processing and communications simply allows for more efficient use of deficient resources [2].

A Sink Node (SN) deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing. While SNs have popularly used for various monitoring purposes such as wild animals, weather, or environments for battlefield surveillance, they also have severely restricted resources such as energy, memory, and computational power. Further, wireless environments give more design challenges due to inherently unreliable communications. A more serious issue is that nodes may be compromised and perform malicious attacks such as packet dropping or packet modifications to disrupt normal operations of a WSN wherein SNs usually perform unattended operations. A large number of SNs deployed in the WSN also require a scalable algorithm for highly reconfigurable communication operations [2]. In this work, we consider a scalable hierarchical structure to deal with a large number of SNs with trust management mechanisms to identify selfish or malicious nodes for trust-based routing in WSNs.

Routing misdirection is an attack whereby malicious nodes advertise false routes to either inject fake traffic into the channel, direct traffic to a dishonest BS or node, exclude part of the network by exhausting its resources or avoid forwarding packets entirely. Such an attack can be countered using authentication, monitoring the network and redundancy techniques [3]. Therefore security in Wireless Sensor Networks is of great importance to ensure the success of an application and secure data transmission. Moreover, analysis of security requirements

gives right directions to develop or implement the proper safeguards against the security violations. The communication among sensor nodes is done by using wireless transceivers due to which they are vulnerable to security attacks. Sensor nodes may also be physically captured or destroyed by the adversaries [4].

We propose an efficient distributed trust model for WSNs for efficient communications. Unlike prior work, we consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node (SN) for WSN applications wherein both social trust and QoS trust are important for mission execution. We apply our hierarchical trust management protocol to trust-based geographical routing as an application. Traditional geographic routing [5, 6] uses geographic location information to select the next forwarding node closest to the destination node, so that a message if delivered successfully may be delivered with the shortest delay. However, in the presence of selfish and malicious nodes, geographical routing may result in low message delivery ratio because the next forwarding node selected may be compromised or selfish, resulting in message losses. Unlike traditional geographical routing, trust-based geographical routing uses both trust and distance as criteria to select the most trustworthy neighbor nodes among those closest to the destination node for message forwarding so that a message may be delivered successfully with a high probability. The key design issues considered include trust formation (i.e., how a peer-to-peer trust value is formed), trust aggregation (i.e., how information is aggregated in parallel), and trust composition (i.e., what trust components are considered and their optimal weights) of the hierarchical trust management protocol and its application to trust based geographical routing.

II. LITERATURE SURVEY

The trust management methods can be classified into two categories: distributive authorization system based on trust chain and network trust evaluation system based on nodes' behaviors [2-5]. (1) In the former system, the authorized individual is allowed to collect all the information of other authorized ones. It checks the consistency through strategy inference engine in light of local policy and authorization requirements. In addition, if a trust chain exists between two strange individuals, the
authorization is able to be relayed by signing indirect objects which have trust rights. That is to say, the authorization individual has rights to deal with its trusted objects. But it is very dangerous for the limited resources of WSNs when the authorization nodes are compromised.

In the latter system, individuals acquire all kinds of related information, including the actions of evaluated individuals, interacting rules and other individuals' opinions. Then, the sensor nodes obtain other nodes' trust value by different computing method in application. This trust management method has advantages of less resources consumption, peer-to-peer structure and no centers. Therefore, trust management schemes similar to the latter one are more frequently applied in the WSNs.

Viljanen et al [6] came up with all kinds of ingredients of trust evaluation after nearly ten years of research on the trust of the network, which has a guiding effect on trust measurement of the sensor nodes in WSNs. Crosby et al. [7] propose a trust evaluation model based on the classical probability model, which uses simple statistical methods to accomplish trust value computation without considering the trust recommendation between sensor nodes. Therefore, it cannot reflect nodes' real-time trust state accurately.

Ganeriwal et al. [8] make a trust evaluation model and uncertainty analysis based on Bayes theory. Because the lack of prior knowledge about wireless sensor networks, the model's subjective assumptions of prior distribution aggravates the uncertainty of trust. These two models both regard the subject fuzziness of trust as the randomness and use pure probability statistic method to assess trustworthiness, which is difficult to obtain prior knowledge from practical application and inevitably result in something unreasonable. In order to deal with the subjective fuzziness of trust evaluation, Tang et al. [9] propose a trust evaluation model based on fuzzy logic, which provides a formalized inference mechanism and does not give specific trust calculation methods. Krasniewski et al. [10] use the base station to make a centralized trust management of cluster head election. If the cluster head is unbelievable, a new one will be elected in another round to avoid effectively malicious or selfish node to act as cluster head. But the centralized trust management model increases the network communication payload and the passive trust decision-making slows down the convergent speed of cluster head election.

Song et al. [11] add trust component to the LEACH algorithm, where nodes select the highest trust value one from their neighbors as cluster head. Although the distributed algorithm in this scheme has high convergent speed, reputation-based trust management may be vulnerable to collusion attacking. TRANS [12,13], which is proposed by Tanachaiwiwat et al., searches and marks the suspicious positions in WSNs
based on the geographic information route. It puts the nodes at the suspicious positions on a black list and broadcasts them to all the other nodes, thereby achieving trust-based secure routing. But there is the possibility that some nodes are misjudged to be malicious because of the abominable channel or compromised nodes. Consequently, it requires a mechanism to allow the nodes in black list to turn into
usable nodes again, whereas the model neglects this point. Hur et al. [12] divide the network into several grids, which accomplishes secure data integration by crosschecking the consistency of nodes' data, but collusion attacks are not able to be resisted very well.

PTM [13], a research sub-item of UBISEC (secure pervasive computing) supported by Europe IST FP6, which builds models mainly in accordance with revised D-S evidence

theory, defines the inter-domain dynamic trust management based on the pervasive environment. The approach makes a strict punishment to malicious actions and has good computing convergence and scalability. But the shortage of the PTM is that it obtains indirect trust value on average without taking the fuzziness, subjectivity and uncertainty into account. Hsieh et al. [14] use cluster-based structure to ensure the security of wireless sensor networks which includes two modules: (1) the dynamic key authorization is adopted to prevent external malicious nodes from entering when a new cluster is established or a new node joins in the cluster. (2) The nodes in the cluster detect each other and different trust computing methods are formulated based on the different roles nodes act as. The approach is difficult to implement and exists weak computing convergence.

Marmol et al. [15] carry out a wide review of different trust models, provide some pre-standardization recommendations and propose an interface proposal for trust models. Lopez et al. [16] list the best practices that are essential for developing a good trust management system for WSN and make an analysis of the state of the art related to these practices. These two references make an excellent summary, propose many profound viewpoints and show an additional insight on the trust evaluation field. In addition, other protocols [12-13] address trust management methods in self-organization
networks from different views.

III. EXISTING SYSTEM

In the existing methods, they used 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. Most existing studies only provide the trust assessment for neighbour nodes. Moreover, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbour nodes.

IV. LIMITATIONS

The major limitation in the existing methods, they may occur DoS attacks which cannot solve the internal attacks occurring during the data transmission in wireless sensor networks. Trust assessment only provide for neighbour nodes that does not solve the trust dynamic problem in the networks.

V. PROPOSED SYSTEM

In this paper, 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. This paper is a multi-hop network which means that the sensor nodes can only directly communication with the neighbour nodes within their communication range. The packets exchanged between any two non-neighbour nodes are forwarded by other nodes. The forwarding node not only can just “pass” the packets from source nodes to destination nodes but also can process the information based on their own judgments. Generally, the trust value is calculated based on a subject’s observation on the object and recommendations from a third party. The third party who provides recommendations is a recommender

5.1 System Architecture

In this paper, we consider a scenario in which all the sensor nodes are randomly deployed without mobility. As shown in Fig. 1, there are three kinds of nodes in the network: subject nodes, recommender and object nodes. If a sensor node A wants to obtain the trust value of another sensor node B, the evaluating sensor node A is named as subject node and the evaluated node B is the object node.

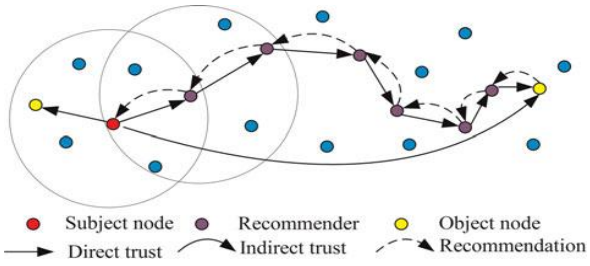

Fig.1 System Architecture

Here, 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.

5.1.1 Direct Trust

Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes.

5.1.2 Recommendation Trust

As mentioned above, since the recommendations from third parties are not always reliable, we need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust.

5.1.3 Indirect Trust

When a subject node cannot directly observe an object nodes' communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes.

Based on [11] and [12], we can conclude that there are three main properties of trust: 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. It is demonstrated in the fig .2 Block diagram of the proposed system.

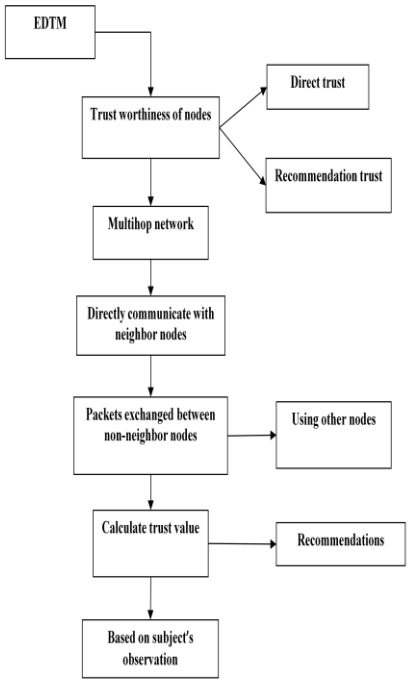

Fig. 2 System architecture

5.2 SYSTEM MODULES

The proposed system contains three modules.

- Network Model
- Calculation of Direct Trust
- Calculation of the Recommendation Trust

A. NETWORK MODEL

In this module, we consider a scenario in which all the sensor nodes are randomly deployed without mobility. If a sensor node A wants to obtain the trust value of another sensor node B, the evaluating sensor node A is named as subject node and the evaluated node B is the object node. This paper is a multi-hop network which means that the sensor nodes can only directly communication with the neighbour nodes within their communication range. The packets exchanged between any two non-neighbour nodes are forwarded by other nodes. The forwarding node not only can just "pass" the packets from source nodes to destination nodes but also can process the information based on their own judgments. Generally, the trust value is calculated based on a subject's observation on the object and recommendations from a third party. The third party which provides recommendations is a recommender.

B. CALCULATION OF DIRECT TRUST

We compose our direct trust by considering communication trust, energy trust and data trust. 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, it is generally known that all communications in WSNs will consume a certain amount of energy to transmit some data packets or any information. If there are malicious nodes in WSNs, the abnormal energy will be consumed or the transmitted data packets will be falsified to conduct malicious attacks. Therefore, 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.

B. CALCULATION OF THE RECOMMENDATION TRUST

The recommendation trust is a special type of direct trust. When there are no direct communication behaviours between subject and object nodes, the recommendations from recommender are always taken into account for trust calculation. However, in most existing related works, the true and false recommendations are not distinguished. How to detect and get rid of false recommendations is important since it has great impact on the trust calculation. When a subject node A wants to obtain the recommendations of an object node B. The subject node A first checks its trust records and then selects a set of common neighbour nodes of node A and node B as the recommenders C1;C2; . . . ;Cn, which have the trust value larger than the threshold 0.5. Subsequently, subject node A transmits a recommendation request message to the selected recommenders

through multi-casting. Obviously, the identity of node B should be added into the recommendation request. Upon receiving a request message, the qualified nodes will reply if they have recommendation of node B. Based on the recommendations, the subject node A filters the false recommendation and compute the recommendation trust of node B.

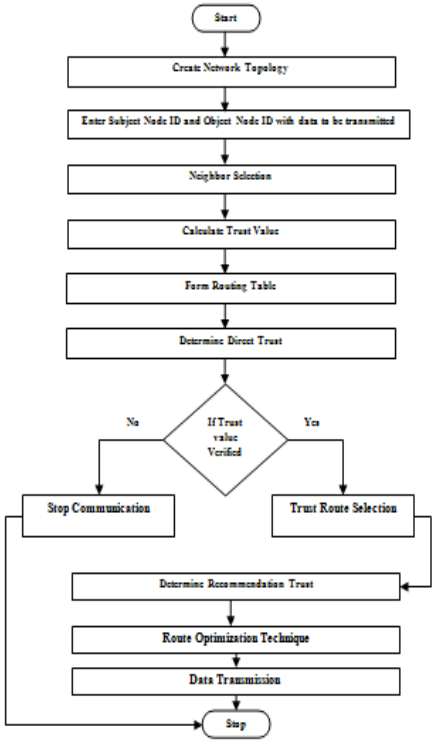

Fig. 3 Flow chart diagram

From the fig .3, Flow chart diagram of the proposed system is clearly describes about the work flow of the paper. Once the network topology is formed, it identifies the subject and node nodes for transmitting data in the networks. Then the neighbour node selection is carried out for making the secure transmission, trust value is estimated in terms of Direct trust and Indirect trust. If the node obtains the trust value within the threshold value, it gets the secure path through trust route selection in the routing topology with help of recommendation trust value and finally the data is transmitted from subject node to object node.

VI. PERFORMANCE EVALUATION

A. Simulation Parameters

The proposed scheme has been implemented on the network simulator ns-2 [11] and the performance compared with some existing mechanisms. The 802.11 MAC layer implemented in ns-2 is used for simulation. Nodes with trust value less than 0.4 are taken as malicious, those 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. The trust value are exchanged in every one-minute interval. Each node has a buffer capacity of 64 packets with secure routing protocol Then, we compare the detection rate of malicious node and the energy consumption of EDTM and NBBTE. The deployment area is set to be $100 * 100$ m .

There are 100 sensor nodes randomly deployed in the sensing area. The malicious nodes 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. The objective trust is calculated 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. Therefore, the subjective trust values are mostly lower than the objective trust values.

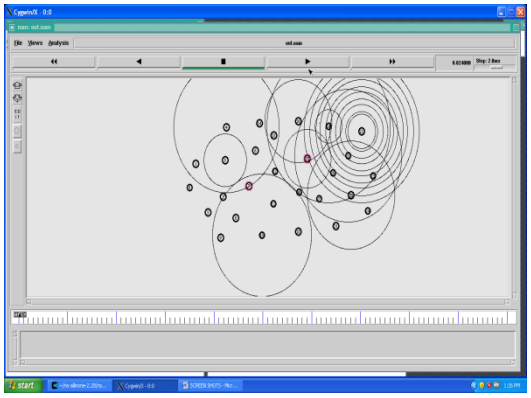

Fig.4 Network topology

Performance Metrics: The metrics used to evaluate performance of proposed approach are residual energy, detection ratio, trust value and recommendation trust value and thus stimulation parameters value are given below:

Table I. Stimulation 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

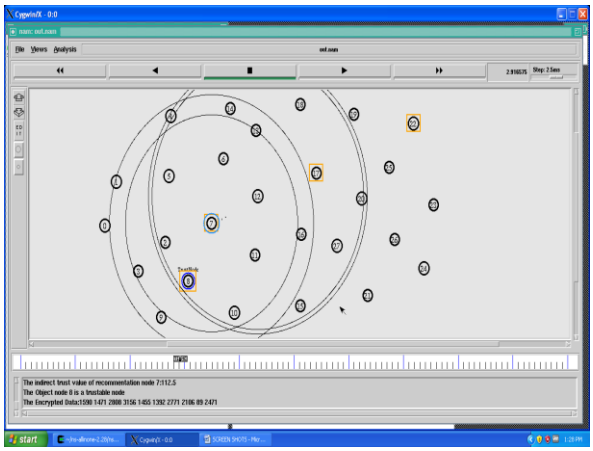

Fig.5 Efficient Distribution Trust Management

VII. SIMULATION RESULTS

We used the performance metrics to validate the proposed algorithm with results obtained in this papers are shown in Figure 6 to 9.

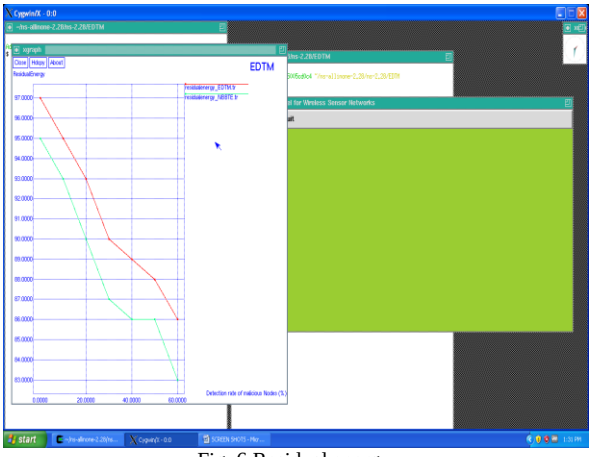

Fig. 6 Residual energy

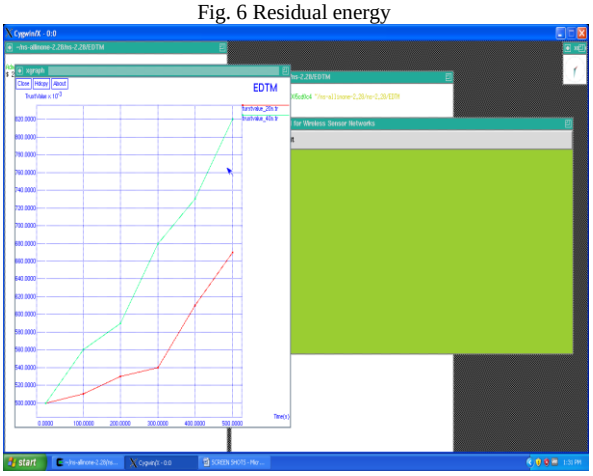

Fig.7 Direct Trust value

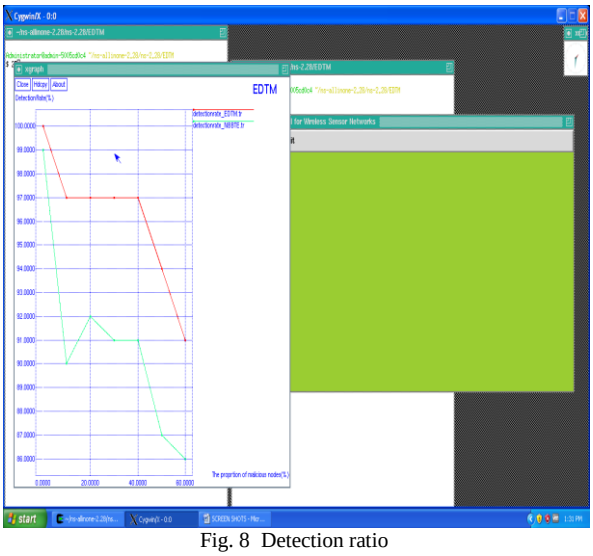

Fig. 8 Detection ratio

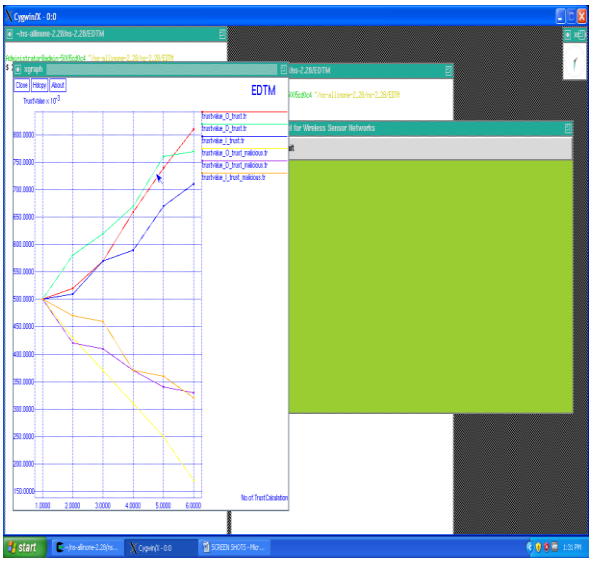

Fig.9 Direct and Indirect trust value

Thus the proposed scheme is very significant and effective when comparing with existing methods.

VIII. 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 paper, 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. Furthermore, the trust propagation and update are studied. Simulation results show that EDTM is an efficient and attack-resistant trust model. However, how to select the proper value of the weight and the defined threshold is still a

challenging problem, which we plan to address in our future research endeavours

.

REFERENCES

[1] H. Chan and A Perrig, "Security and privacy in sensor networks," Comput., vol. 36, no. 10, pp. 103–105, Oct. 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 J. Sel. Areas Commun., 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 Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 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," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.

[5] 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.

[6] 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.

[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, vol. 11, pp. 1345–1360, 2011.

[8] G. Han, Y. Dong, H. Guo, L. Shu, and D. Wu, "Cross-layer optimized routing in WSN with duty-cycle and energy harvesting," Wireless Commun. Mobile Comput., 3 Feb. 2014, DOI: 10.1002/wcm.2468.

[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 Trans. Internet Inf. Syst., vol. 6, pp. 2992–3007, 2012.

[10] 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.

[11] 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.

[12] A. Josang, "An algebra for assessing trust in certification chains," in Proc. Netw. Distrib. Syst. Security Symp., 1999, pp. 1–10.

[13] W. Gao, G. Zhang, W. Chen, and Y. Li, "A trust model based on subjective logic," in Proc. 4th Int. Conf. Internet Comput. Sci. Eng., 2009, pp. 272–276.

[14] M. Chen, Y. Zhou, and L, Tang, "Ray projection method and its applications based on Grey Prediction," Chinese J. Statist. Decision, vol. 1, p. 13, 2007.

[15] 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.

[16] E. Elnahrawy and B. Nath, "Cleaning and querying noisy sensors," in Proc. 2nd ACM Int. Conf. Wireless Sens. Netw. Appl., 2003, pp. 78–87.

[17] M. Rabbat and R. Nowak, "Distributed optimization in sensor network," in Proc. 3rd Int. Symp. Inf. Process. Sens. Netw., 2004, pp. 20–27.

[18] 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.