Middle-East Journal of Scientific Research 24 (S1): 117-123, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.S1.26

Efficient Distributed Trust Model for ADHOC Sensor Networks to Improvesecurity

[1]*Sarathkumar Ragothman and A. Nandini*

[1]M.E. Applied Electronics, Saveetha Engineering College, Chennai, India
[2]Department of ECE, Saveetha Engineering College, Chennai, India

Abstract: With advancement in wireless technologies and mobile devices, Wireless Ad hoc Networks have become popular in communication technology in many environments. In communication, security is a major concern. The security is a key point for data transferring between source and object node, it involve packet loss, delayconstraint, attacks etc. Key management is one of the security techniques for authentication, so that intended receiver only decrypts the message of sender. It enhances security by transferring data between intended receivers, but it may drop the packet in the network by malicious node. In order to transfer the data in the secured path without the data loss, Trustmodel mechanisms have been suggested for Wireless Sensor Networks(WSNs). The trust values are calculated from communication modeling behaviorof nodes.In this, Efficient Distributed TrustModel (EDTM) for WSNsis proposed and it can evaluate trustworthiness ofsensor nodes more precisely.Simulation results show that other similar models outperform with EDTM.

Key words: WSN · EDTM · Trust models · Energy efficient

INTRODUCTION

Wireless Sensor Networks (WSNs) is a self-configured and infrastructure-less wireless networks to monitor environmental or physical conditions. WSNpass their data to a main location or sink cooperatively through the network, which can be observed and analyzed. By injecting queries one can retrieve required information from the network. The hundreds of thousands of sensor nodes make a WSN. Each node can communicate among them using radio signals. Every node in a wireless sensor network (WSN) is inherently resource constrained: they have limited processing speed, storage capacity and communication bandwidth. After deploying the node, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them.

WSN is an emerging technology used widely in major areas like healthcare monitoring [1], smart power grid [2], emergency response [3], habitat monitoring traffic management, battlefield surveillance etc. Nature of sensor network such as wireless as well as resource constraint makes a medium for intruders like malicious attackers in a network. However security is indeed for the secure application of wireless networks. Security mechanisms proposed to avoid security threats e.g., cryptography, authentication, confidentiality and message integrity such as message replay and eavesdropping. But malicious attacks and denial of service (DoS) attacks are security vulnerabilities for these security threats. Attacks are classified mainly as internal andexternal attacks.

Security mechanism so far proposed is used to protect from external attacks only, but it does not effectively solve the internal attacks. For such attack trust values of the participating nodes are calculated based on trustworthiness of all other node.A major aspect of wireless sensor network is to minimize the power consumed by the nodes present in the network. The radio subsystem which transmits the date to the neighbor communicating node consumes the largest amount of power. To minimize the power consumption in the radio subsystem, wakeup concept is used. The radio network is in wakeup when it sends the data over the network. Then the nodes enter into a sleep mode. An algorithm is loaded in a node to wakeup a node while transmitting based on the sensed event. Furthermore, it is important to minimize the power consumed by the sensor itself.

There are several trust models have developed to build trust values within sensor nodes [4]. The initial trust model for WSNs is a distributed Reputation-based Framework for Sensor Networks (RFSN) [5]. The blocks of RFSN are Watchdog which monitors communication

Corresponding Author: M.E. Applied Electronics, Saveetha Engineering College, Chennai, India.

behavior of neighbor nodes and Reputation system to maintain the reputation of a sensor node. This reputation value is need for calculating the trust value of a node. But, in RFSN recommendation trust from neighbor node is ignored, while direct trust only considered and calculated.

In order to consider recommended trust as well as direct trust to have good trust relationship with sensor nodes proposed Parameterized and Localized trUst management Scheme (PLUS) [6]. Another trust based algorithm is Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm (NBBTE) is proposed based on D-S belief theory [7]. NBBTE identifies various trust factors for the communication behaviors between two neighbor nodes in the network. Now considering the recommendation values of the neighbor nodes, D-S evidence theory method is used to obtain trust value instead of simple weighted-average one. NBBTE is more advantage; hence it used as comparing method.

The paper is sectioned as follows: In Section 2, network scenario model is discussed. In Section 3, the EDTM overview is explained. In Section 4, the EDTM trust values and its definitions are provided. In Section 5, the performance of the EDTM is evaluated. Section 6 concludes the paper.

Network Model: In general, WSN nodes are deployed randomly with high mobility. The nodes are of three kinds, they are subject, object and recommender node. Suppose a sensor node X obtains the trust value of another node Y, then the node X is denoted as subject node and the node Y is denoted as target node. If subject and target nodes are within the range then single hop communication occurs. In multi-hop network, in which sensor nodes (subject node) can directly communicate with the neighbor nodes within the network range. The neighbor nodes are responsible for packet exchange between end nodes. So, it passes the packets from the source node to destination node (target node) also process its information. The trust value is calculated based on a node X (subject node) observation on the node Y (target node) and recommendations from a third party. The recommender is a third party node which provides recommendations.

Network Attacks: Data plane attacks in a network is a malicious node attacks in WSNs, such as Sybil attack, wormhole attack, DoS attack, node replication, attacks on Information, etc. Such attacks are vulnerable to trust model like as bad/good-mouthing attack and on-off attack. Malicious nodes intentionally provide dishonest recommendation to neighboring nodes in a bad-mouthing attack.

However, under bad-mouthing attack recommendations cannot reflect the real opinions of the recommender. Whereas attacker node intentionally provides higher trust value for malicious nodes is a good-mouthing attack

EDTM Overview: EDTM has two main components is shown in Figure 1; they are one-hop trust model and multi-hop trust model. It includes six components such as directtrust module, recommendation trust module, indirect trustmodule, integrated trust module, trust propagation moduleand trust update module. When a subject node X wants toobtain the trust value of an object Y, it checks its list of neighbor nodes. If the object node Y ID is in thelist, thenthe one-hop trust model is triggered. Or else, the multi-hop trust model is initiated.

In the one-hoptrust model, if the trust is calculated from direct experiences based on node Y's with node X completely, this model is direct trust model. If not, the recommendationtrust module is used. In the multi-hop trust model, recommendations from other nodes about the object node Y received by thesubject node Xand indirect trust model can beestablished.

Direct trustto evaluate sensor nodes is not accurate for malicious attacks. Hence, to improve the trust evaluation the recommendationfrom other sensor nodes are needed. If the number of communicationpackets is too small, it is difficult to decide whether an object node is good or badbased on few interactions. Therefore, in the one-hoptrust model, it defines a threshold of communication packetsTh-num. The direct trust is calculated, if communication packets between the subjectand object nodes are higher than the Th-num. Otherwise; the recommendationsare needed for the object's trust evaluation from the recommenders.

Trust Values: This section, presents procedure for the trust calculation in details.

Direct Trust: Direct trust calculated by considering communication trust, energy trust and data trust. The sensor nodes perform their tasks by communicating with neighbor nodes. This communication behaviors are always evaluates whether the sensor node is normal or not. Due to the nature of wireless communication, the communications between sensor nodes are unstable and

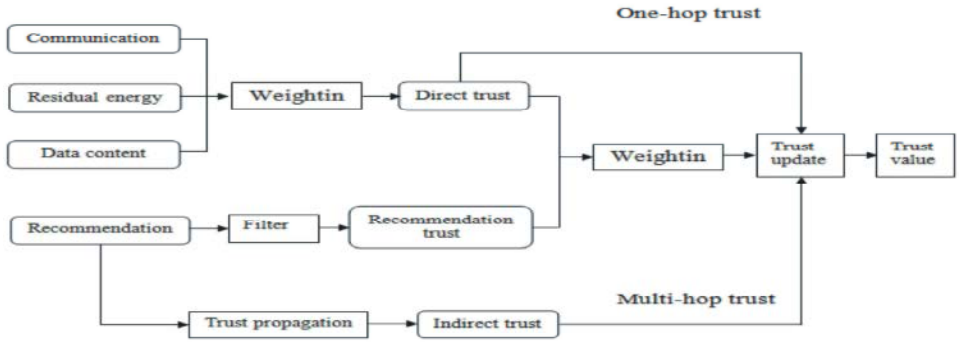

Fig. 1: An EDTM

there are many reasons resulting in the packets loss in wireless communication. The malicious nodes in the network results unsuccessful communication or unstable communication channel. In addition to communication behavior, amount of energy to transmit some data packets or any information is calculated. In case of malicious nodes in WSNs, the abnormal energy will be consumed by nodes due to false update or the transmitted data packets will be falsified to conduct malicious attacks. Hence communication, energy and data trust are defined in EDTM. In communication trust, sensor node can cooperatively execute the intended protocol. In energy trust a sensor node is competent in performing its intended functions or not. In data trust, assessment of the fault tolerance and consistency of data are considered. It affects the trust of the sensor nodes that create and manipulate the data.

Recommendation Trust: When there are no communications behavior directly exists between subject and object nodes, the third party recommendations from recommender node taken into account for trust calculation. If, subject node X transmits a recommendation request message to the selected neighbor recommenders through multi-casting. Obviously, the identity of object node Y should be added into the recommendation request. Once receiving a recommendation request message from recommenders, the qualified nodes will reply if they have recommendation of node Y. Based on the recommendations, the subject node X filters the false recommendation and compute the recommendation trust of node Y.

Indirect Trust: WSNs are multi-hop networks are spurred, when there are no direct communications between subject and object nodes. The calculation of indirect trust includes two steps: 1) find multi-hop recommenders between subject and object nodes and 2) the trust propagation that is computing the direct trust. The path between the subject nodes to the object node established by the recommenders is termed as Trust Chain.

Based on the location information of sensor nodes in the network, it observed three different kinds of ways for choosing the recommender in the network:

- Choose the closest recommender to the object node to save energy consumption
- Choose the highest trust value to guarantee the reliability of Trust Chain
- Choosean optimal Trust Chain by both considering the distance information and the trust value.

Performance Evaluation: Simulation results and analysis shows the performance of EDTM based on parameters, like trust value of nodes. Then, the energy consumption and the detection rate of malicious node are compared for EDTM and NBBTE. In this scenario, sensing area has 50 sensor nodes deployed randomly.

Trust Analysis: The direct trust, indirect trust and communication behavior between source and object node are considered as a major trust analysis. Figure 3 shows that direct trust between source node X and object node Y has high probability of trust for normal nodes than malicious nodes in the network.

Similarly, indirect trust is simulated in the simulator tool and it is observed that the malicious node in the network has low probability of trust value compare to normal nodes as shown in figure 4. It explains the data can take the path with high probability of trust value and so security of the data is achieved.

Performance of EDTM: From Figure 5, performance evaluation of direct and indirect trust in EDTM is analyzed. In this scenario, network with malicious nodes and without malicious nodes are considered.

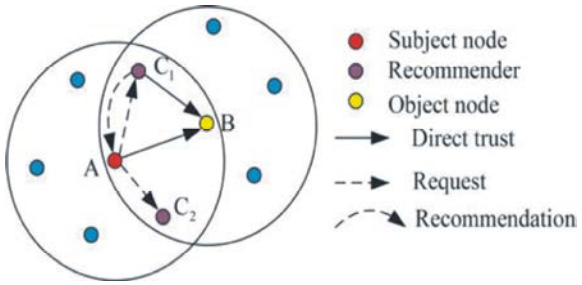

Fig. 2: Calculation of the recommendation trust

Fig. 3: Direct trust with and without malicious node

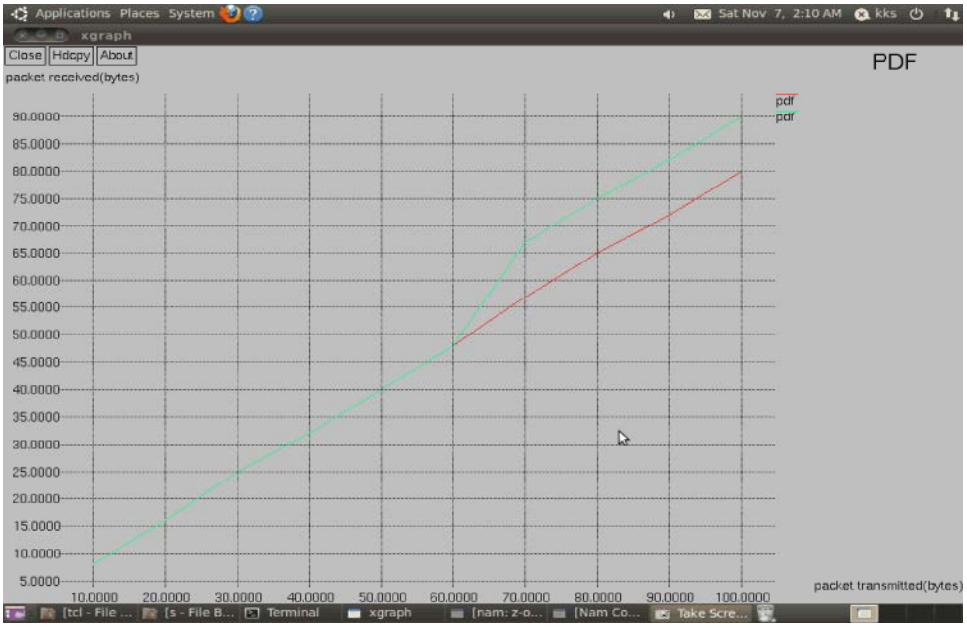

Fig. 4: Indirect trust with and without malicious node

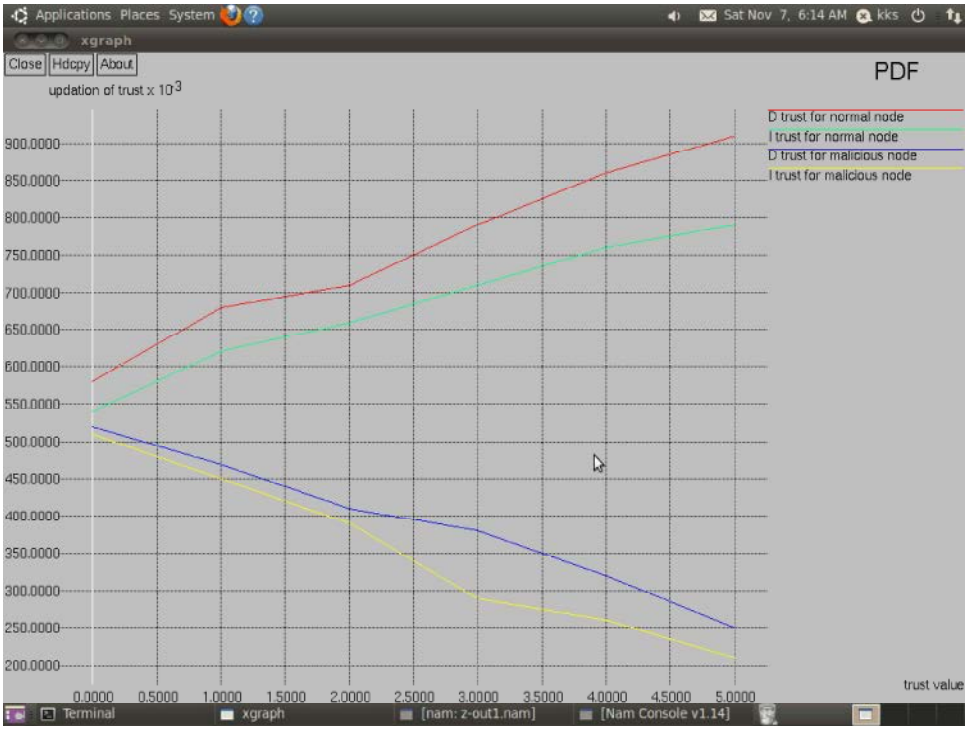

Fig. 5: Trust value update

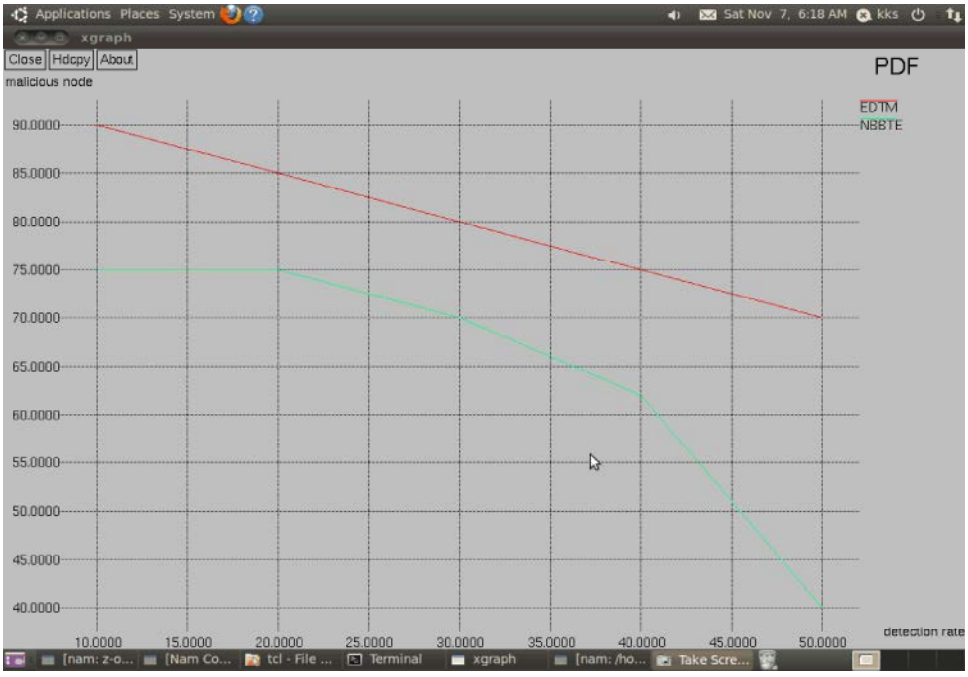

Fig. 6: Malicious node detection rate

The trust value has high probability in the case of network with normal nodes (non-malicious node). The probability is low for the case of network with malicious nodes. In similar way, performance is compared with direct and indirect trust and it shows that EDTM is performed better for the both cases of with as well as without malicious node in the network.

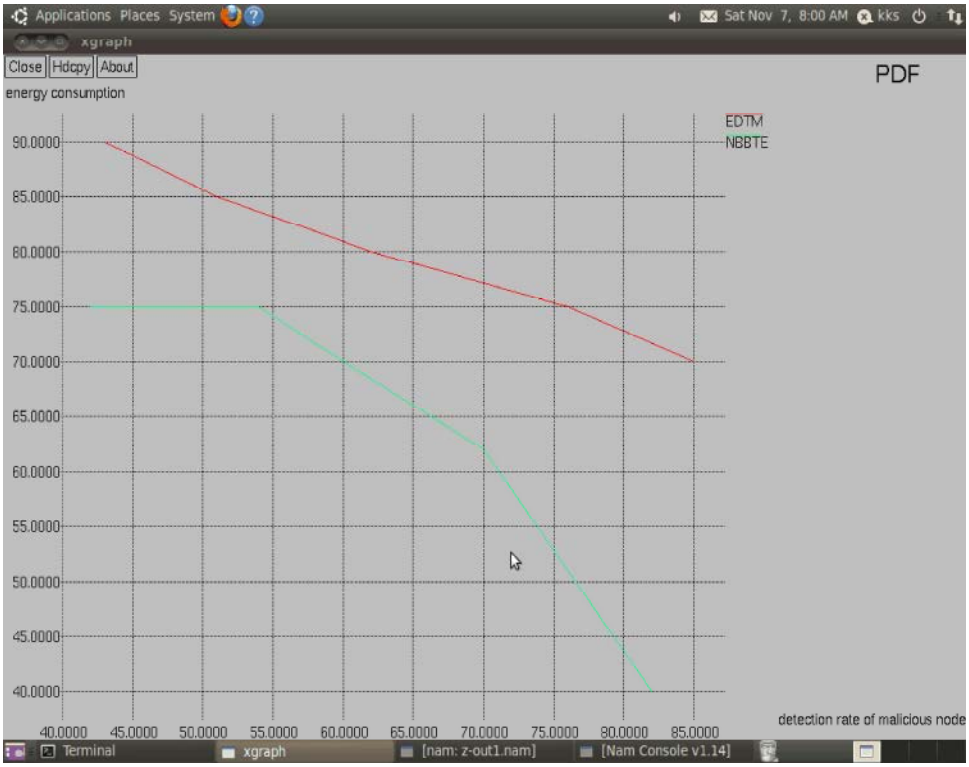

Fig. 7: Comparison of energy consumption

Detection Rate of Malicious Node: The malicious attacks are data forgery attack, bad/good mouthing attack, selective forwarding attack, DoS attack, on-off attack. The detection rate is given as ratio of number of malicious node detected to the number of malicious node in the network.

Detection rate is analyzed by introducing malicious node in the network and computing EDTM and NBBTE. NBBTE mostly vulnerable to malicious node attack, so detection rate decreases rapidly with increase of number of malicious nodes in the network. In Figure 6, it shows that the performance of the EDTM is better than that of NBBTE. Malicious node in the network decreases the performance of the network hence EDTM is used to increase the performance.

Comparison of Energy Consumption: Energy consumption of the malicious node in the network is compared using EDTM with NBBTE method by increasing the malicious node at the rate of 5%. In EDTM, each node stores the information of the neighbor nodes alone. Carrying the neighbor information leads to low power consumption. While, in NBBTEeach node storesrouting information of every other node in the network. By varying the malicious nodes in the network, the energy consumption is measured. In this EDTM outperforms more efficient compare to NBBTE is shown in Figure 7.

CONCLUSION

A trust calculation is effectively used in WSNs to reduce data-plane attacks. Trust model can be used in major applications like secure key exchange, data aggregation and secure routing. WSN is a wireless technology, to improve its security it identify a distributed trust model which can monitor every other node in the network with the help of neighbor nodes. In efficient and distributed trust model called EDTM isused to for handling trust values in an efficient way. In EDTM the trust values of direct trust, indirect trust and recommendation trust are observed. Simulation result analyzed that EDTM send the data through highly recommended path and reduce the data plane attack. However, the trust value has been updated; still defining the threshold level for the trust is a challenging one in the network.

REFERENCES

1. Huang, Y.M., M.Y. Hsieh, H.C. Chao, S.H. Hung and J.H. Park, 2009. "Pervasive, secure access to a hierarchical-based healthcare monitoring architecture in wireless heterogeneous sensor networks, " IEEE J. Sel. Areas Commun., 24(7): 400-411.
2. Gungor, V.C., L. Bin and G.P. Hancke, 210. "Opportunities and challenges of wireless sensor networks in smart grid, " IEEE Trans. Ind. Electron., 57(10): 3557-3564.
3. Chan, H. and A. Perrig, 2003. "Security and privacy in sensor networks," Comput., 36(10): 103-105.
4. Han, G., J. Jiang, L. Shu, J. Niu and H.C. Chao, 2014. "Managements and applications of trust in wireless sensor networks: A Survey," J. Comput. Syst. Sci., 80(3): 602-617.
5. Ganeriwal, S., L.K. Balzano and M.B. Srivastava, 2004. "Reputationbased framework for high integrity sensor networks," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., pp: 66-77.
6. Yao, Z., D. Kim and Y. Doh, 2008. "PLUS: Parameterized and localized trust management scheme for sensor networks security, " in Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst., pp: 437-446.
7. Feng, R., X. Xu, X. Zhou and J. Wan, 2011. "A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory, " Sensors, 11: 1345-1360.