Analysis of Trust in Wireless Sensor Networks

N.Karthik,
Assistant Professor, Department of Information Technology,
Adhiparasakthi College of Engineering, Kalavai, Tamilnadu, India.
Email id: nkarthikapce@gmail.com

J.Karthik,
Research scholar, Department of Computer Science and Engineering,
St.Peters University, Chennai, Tamilnadu, India.
Email id: karthikvalavan@gmail.com

M.Ashwini,
B.Tech (IT),
Adhiparasakthi College of Engg., Kalavai, Vellore, Tamil nadu, India.
Email: ashwinichinna03@gmail.com

ABSTRACT

Trust is an important factor in Wireless Sensor Network (WSN) that enables the sensor node to cooperate each other for their application. It makes the nodes in the wireless sensor networks to cope with uncertainty caused by the other nodes in the network. Managing the trust in the wireless sensor network is highly challenging task due to resource constraints and network dynamics. To have a secure communication, it is necessary that a node in the network should analyze the trust level of the communicating node in the network. In WSN, an untrustworthy can cause damage to the sensed data in terms of reliability, quality and integrity. In this work, we analyze various trust computation methodologies and components for finding trust. In addition to that, we also highlight the trust metrics, and terminologies in WSN.

Keywords: Trust Computation, Trust Propagation, Trust Prediction, Trust Maintenance, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor network is a distributed network. The wireless sensor network has ability to setup huge amount of nodes that assemble and configure themselves. The idea behind wireless sensor networks is that, the potential of each individual sensor node is restricted, the aggregate power of entire network is sufficient for the required mission. Many parts are embedded in each sensor network, like radio transceiver, microcontroller, electronic circuits and an energy source as battery.

Wireless sensor network is more expensive, high power consumption, software programmable, data acquisition, bidirectional communication, scalability, responsiveness, reliability and easy to use [1]. Wireless sensor network generally consists of a base station, number of sensors connected via a radio link. The major benefit of the system is that they perform internetwork processing to reduce large streams of raw data into useful aggregated information. Wireless sensor network is used in many real time applications such as environmental monitoring, industrial control and monitoring, home automation, military surveillance, patient monitoring etc.,

Trust in network is more difficult, when it is larger. Fewer links may be better to make one more dependent on its network and thus more trustworthy. The trust is the level or degree of confidence or belief that a node can have on another node. Trust management in WSN is used in assessing the quality of the sensed data, security services like access control, authentication, uncertainty and malicious node detection. Trust development in the network has been implied as good security method for resource reserved wireless senor networks. Developing the trust worthy framework for the wireless network makes the security stronger, reliable and more efficient [2].

Organization of the paper

The discussion of the paper is as follows: section 2 deals with the characteristics of trust in WSN. Some terminologies are introduced in Section 3. Basic components in trust evaluation and types of trust computations are explained in section 4. Section 5 deals with representation of trust values and states of nodes in WSN. Finally some concluding remarks and future works are given in section 6 and section 7 respectively.

II. CHARACTERISTICS OF TRUST IN WSN

1. *Dynamic*: It may increase or decrease by time based on successful and unsuccessful interactions.
2. *Subjective*: Based on observations made at specific situation.
3. *Reflective*: Self-trust
4. *Intransitive*: If node A trusts node B, node B trusts node C. it is not necessary that node A trusts node C.
5. *Asymmetric*: Two nodes do not have similar trust
6. *Not absolute*: Node A do not trust node B for any action it chooses but it will trust for specification
7. *Trust is linked with risk*: There is no reason to trust if there is no risk involved.
8. *Mutual causality*: Interactions between nodes influence their behavior and lead to updating their trust value by recommendation exchanges and direct observation.
9. *Auto catalysis*: Nodes exchanges references about other nodes
10. *Morphogenetic change*: Networks with no infrastructure, such as wireless sensor networks are always confronted with random conditions.
11. *Cooperative*: The nodes deployed in environment are cooperative to each other by exchanging information.

III. TERMINOLOGIES OF TRUST MANAGEMENT

Trust: Trust is the degree of belief is the competence of an entity to act as expected such that this belief is not a fixed value associated with the entity but rather, it is subject to the entity's behavior and applies only within a specific context at a given time.

Reputation: If an entity is an expectation of its behavior based on other entities observations or information about the entity's past behavior within a specific context at a given time.

Reliability: The trusting beliefs in the network will increase if the network is reliable, generating a willingness to depend on that network, that is persuade nodes to interact with the network, share resources and information.

First hand information: A node will observe a neighboring node's behavior and build a reputation for that node based on the observed data. The neighboring node's transactions data are direct observations referred as first hand information.

Second hand information: Second hand information in trust modeling is information provided by other nodes. This source of information is referred as second hand information. It consists of information gathered by nodes as first-hand information and converted into assessment.

IV BASIC COMPONENTS IN TRUST EVALUATION

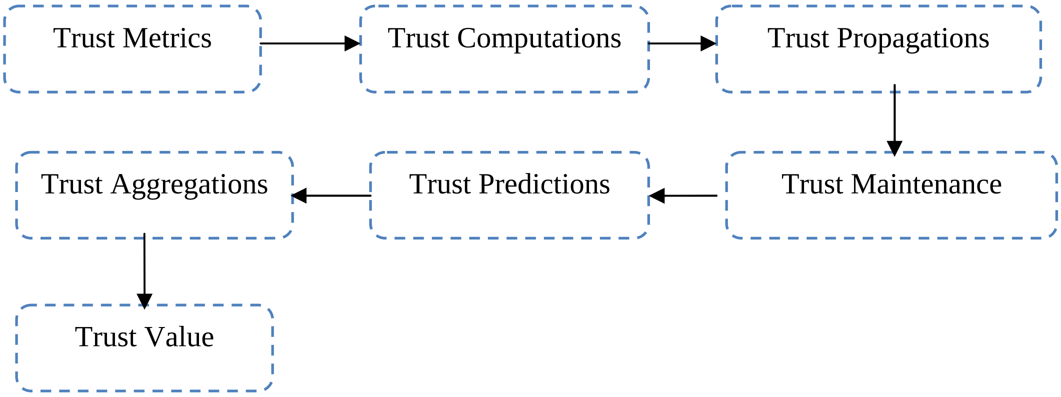

Fig 1: Basic components in Trust Evaluation

A. Trust Computations:

The trust computations in Ad hoc networks may be classified into distributed and centralized trust computations. In distributed trust computation, every node in the sensor network computes the trust value of other nodes directly either by experience or observations. In centralized trust computation, the third party or central trusted agent in the network aids the node for trust evaluation. Sometimes the hybrid trust calculation may be followed by the sensor node in the network in order to have clear view about the communicating node in the network. The hybrid trust value of the node is computed by direct experience and by getting recommendations from the other nodes in the network.

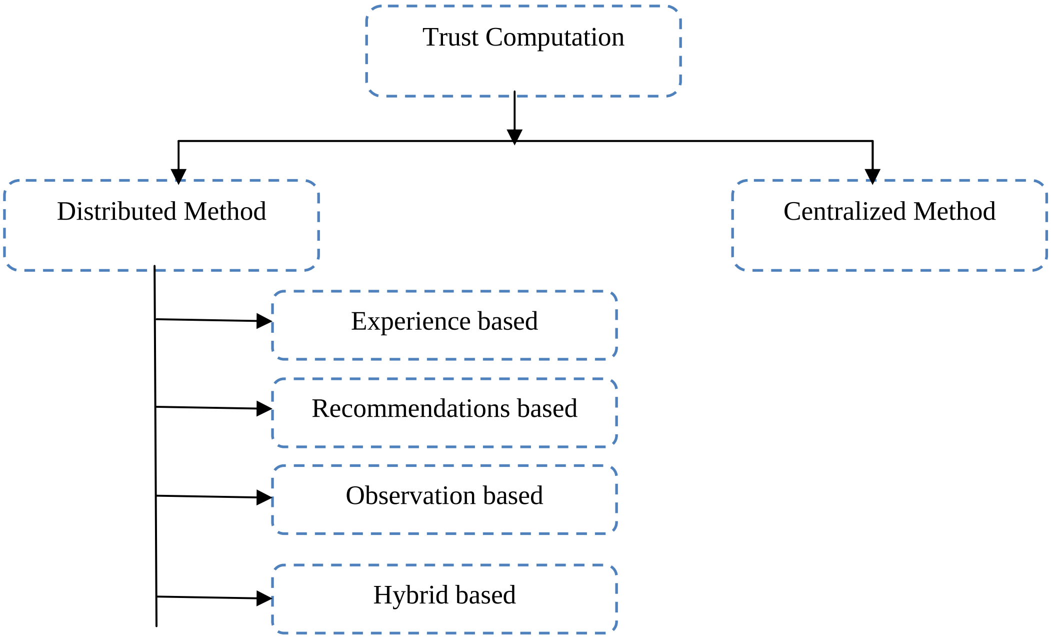

Fig 2: Types of Trust Computation

The availability of remaining resources in the node and the type of application decides the type of trust computation. However most of the trust computation methods are distributed in nature. Because the centralized trust computation method suffers from single point of failure.

B. Trust propagation:

Trust value of the node must be propagated along the network when a node seeks the opinion or trust value in terms of recommendations about the other nodes in the network. It is also called as Indirect trust. The major factor to be considered for the propagation is the secure path / protocol and the cooperation among the nodes in the network for exchanging the opinions / recommendations about the other nodes in the network. For example we may use Trusted AODV protocol for exchanging the trust value / recommendations about the other nodes. Sometimes, the request for opinions issued by the trust requestor may broadcast to other nodes in the network. Upon receiving the request by the nodes, the trust provider will forward the recommendations about the target node through intermediate hops. Here selection of intermediate hop / path is very important for forwarding the trust value to the trust requestor.

C. Trust Aggregation:

When the trust requester issues the trust request about the target node in the network, the trust request will be forwarded to multiple paths in order to reach the multiple nodes in the networks. Upon receiving the trust request from the trust requestor, every node will send its opinion about the target node to the trust requestor. The multiple versions of a trust state / recommendation of the target node is received at the trust requestor. The aggregation operation must be performed at the trust requester in order to obtain a single trust value for the target node [3]. Trust requester must ensure about the trusted path in which the recommendations / opinions are forwarded. If the path contains any malicious node, it can alter the trust information which results an uncertain condition about the target node.

D. Trust Predictions:

It is a method of forecasting the behavior of nodes using present and past history of the nodes. Sometimes, the trust prediction may include the recommendation / opinions collected from the other nodes. It helps the nodes in the network to be act carefully in order to avoid potential problems or danger while communicating with the strange node. The accuracy of the trust value predictions of target node depends upon the number samples available at the moment of prediction / forecasting.

E. Trust Maintenance:

The Trust value of the target node is stored in the trust requester node for further processing and consequent action. The trust value maintenance includes the recording of direct and indirect trust values of the target node in the form of table at the trust requester node. The memory requirement for storing / maintaining the trust value at trust requestor node is explained in [4]. Trust value of the target node in WSN can be represented as continuous values in the range of (-1 to +1) or trust states. The benefit of using trust state is that it allows the nodes to propagate the trust state easily then propagating the decimal value due to the energy constraints in sensor node.

The mobility of the node, network density and link breakage between the nodes in the network have some influence on trust computation, propagation, aggregation and prediction [5].

V. REPRESENTATION OF TRUST STATES AND VALUES

The trust value of the node in the WSN can be characterized as a continuous variable and it has the value ranging from -1 to +1. In general the trust value of the node in the network can be represented as a numeric value. In our previous work, we have represented the trust value of the node as trust state which can be further understood as trusted, untrusted and uncertain states. The trust states and its respective trust values are shown below.

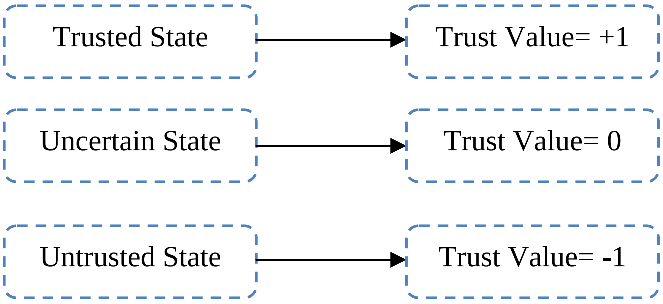

Fig 3: Trust States and its Trust Values

VI. CONCLUSION

The objective of this work is to provide the concept of trust to network developers with multiple perspectives that should be considered in developing a trust model for the highly dynamic environment and to provide deep and accurate mechanism for the computation of trust. We have started with trust definition, followed by trust computation methodologies used for the evaluation of trust in WSN. We also analyzed the trust propagation, prediction and trust computation.

VII. FUTURE WORK

The existing works and proposals lack completeness based on our observation. In near future, we are going to design a new trust system / model for WSN by considering the constraints, nature of network and the type of application, where the node can be deployed and this will be tested in real time applications.

VIII. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubrarnanian, and E. Cayirci, “Wireless sensor networks: A survey,” Computer Networks, Elsevier Science, 38(4), pp. 393-422, 2002.

[2] N.Karthik, J.Karthik, “Trust Worthy Framework for Wireless Sensor Networks”, International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 5 No. 05 May 2014 pp 478-480 ISSN : 2229-3345.

[3] N.Karthik, V.R.Sarma Dhulipala, “Trust Calculation in Wireless Sensor Networks”, IEEE International conference on Communication, Electronics and Technology, IEEE ICECT’11.

[4] V.R.Sarma Dhulipala, N.Karthik, R.M. Chandrasekaran, “A Novel Heuristic Approach based Trust Worthy Architecture for Wireless Sensor Networks”, Wireless Personal Communication, May 2013, Volume 70, Issue 1, pp 189-205.

[5] Kannan Govindan, Prasant Mohapatra Tarek F. Abdelzaher,” Trustworthy Wireless Networks: Issues and Applications”, invited paper in International Symposium on Electronic System Design, 2010.