Journal of Network and Computer Applications 62 (2016) 75–87

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Sociopsychological trust model for Wireless Sensor Networks

Heena Rathore *, Venkataramana Badarla, George K J

Indian Institute of Technology Jodhpur 29, Bhairav Colony, Sector-3 Udaipur, Rajasthan 342011, India

ARTICLE INFO

Article history:
Received 12 August 2014
Received in revised form
7 September 2015
Accepted 20 September 2015
Available online 22 December 2015

Keywords:
Sociopsychological trust model
Wireless Sensor Network
Security
Ability
Benevolence
Integrity

ABSTRACT

Trust plays a crucial role in establishing and retaining relationships. Sociopsychological analysis identifies three major constructs, such as ability, benevolence and integrity, upon which trust is being built up. On a similar note, in a Wireless Sensor Network (WSN), it is indispensable to have trust among nodes since nodes collectively sense physical parameters and send them to the base station. The nodes, however, can behave fraudulently and send bad information, mostly due to hardware and software faults. Taking inspiration from the sociopsychological account, the present paper introduces a novel model for computing trust of sensor nodes. Additionally, the immune inspired model is suggested for removing fraudulent nodes whose trust ratings fall below the threshold. Roles of the three factors, viz. ability, benevolence and integrity, are examined in WSN domain. The proposed model proves itself to be more advantageous than other methods that adopt machine learning and neural network models in performance metrics such as detection time, reliability, scalability, efficiency and complexity. Proposed work has been implemented on LabVIEW platform and the results substantiate the reliability of the proposed mathematical model.

1. Introduction

Trust has always been a major concern for a variety of fields such as sociology, psychology, philosophy, computer networks and social networks. It is an elusive notion, mostly because of its subjectivity and context-specificity. In an organisation which incorporates people from diverse backgrounds into its network, each member has to trust others to accomplish one's own personal goals and the collective goal of the organisation. Trust plays a decisive role in establishing and sustaining harmonious relationship among the members and facilitates rational predictions of the dynamics of relationship within the organisation.

In a Wireless Sensor Network (WSN), where the sensor nodes coordinate with each other for monitoring environmental conditions and sending the data to the base station, it is essential that trust is established among the nodes so that they could confidently rely on other nodes and send the data faithfully. Trust plays a vital role in WSN where data authenticity is an important factor. Nevertheless, owing to certain hardware and software faults, nodes can behave fraudulently and send fraudulent information. The errors that take place while sending information can decrease the trust ratings of the sensor nodes. Nodes with lesser trust ratings should be removed from the network as it reduces the data authenticity and credibility.

The present paper provides a novel approach for calculating trust of sensor nodes. The paper introduces for the first time sociopsychological norms for computing the trust of the sensor nodes. The three factors namely ability, benevolence and integrity are used for computing the trust of the nodes. For the removal of those nodes which are identified as fraudulent from the sociopsychological trust model, immune model inspired from human immune system is used. The paper organisation is as follows: Section 2 presents an overview of the prevailing trust models which justifies the significance of the proposed model. The section also explicates the sociopsychological account of trust and analyses the major concepts that are related to trust. Section 3 has two parts. The first part proposes the model that can be used in WSN for generating trust ratings of the sensor nodes and the second part proposes the model for removing the nodes whose trust ratings falls below a particular threshold. Discussing the experimental results, Section 4 evaluates the efficiency of the proposed work. Section 5 presents the critical appraisal of the proposed model with other trust models. Finally, Section 6 concludes the discussion.

2. Related work and background

2.1. Trust models in WSN

Nodes, while sensing data, can produce ratings that are based on direct observation (known as firsthand information) and indirect observation (known as secondhand information). Paying

* Corresponding author. Tel.: +91 9413695821/+91 316730 0382.
E-mail addresses: heena7sept@iitj.ac.in (H. Rathore), ramana@iitj.ac.in (V. Badarla), kjg@iitj.ac.in (G. J).

http://dx.doi.org/10.1016/j.jnca.2015.09.009
1084-8045/

attention to the both, Momani et al. (2010) present a survey of trust models in different network domains. Several techniques such as ratings, weightings, probability, Bayesian network approach, game theory approach, swarm intelligence, neural network method and fuzzy logic are used in assessing trust factor of sensor nodes (Momani and Challa, 2010). In the above list, ratings and weightings methods use very simple mathematical equations both on firsthand information and secondhand information. Liu Zhiyuan et al. (2011) employ Bayes' rule as the criterion for computing trust ratings. The framework proposed by them was so generic that it allows enough room for adding and/or deleting components in addition to direct observation and indirect observation (Zhiyuan et al., 2011). Shigen Shen et al. (2013) propose the game-theoretical approach in determining fraudulent nodes (Shen et al., 2013). Yenumula et al. (2012) use fuzzy logic approach and calculate the reputable path in the light of three principles, namely fuzzy matching, inference and combination (Reddy, 2012). Marmol et al. (2011), using swarm intelligence approach, try to detect the most trustworthy path that leads to the most reputable node in WSN. It calculates the shortest path and assigns higher ratings to those nodes which come in the path (Marmol and Perez, 2011). Curiac et al. (2007) use neural predictors to calculate trust ratings which is performed in the light of the information collected from the network of neighbouring nodes and the information received from them in the past.

In our earlier work (Rathore et al., 2013), we have used machine learning model for detecting fraudulent nodes. The model employs techniques such as K-means, Support Vector Machine (SVM) and uses Anomaly Detection Engine (ADE) for the detection. However, the focus of the work was confined to temporal information alone (Rathore et al., 2014). Likewise, the idea of trust ratings was not considered in the study. Nevertheless, the study finds that it is not enough to depend on any single trust component in determining the trustworthiness of nodes in WSNs. Considering the possibility that relying on a single component might mislead the judgement, it is suggested that more than one component should be considered while computing trust (Momani et al., 2008). Proposing sociopsychological module, the present paper introduces a novel technique for calculating the trust ratings of the sensor nodes. Among other advantages, the module pays due attention to temporal and spatial information alike.

2.2. Trust: the sociopsychological account

The subsection gives the insights and background on sociopsychological norms that are considered for building of trust in society.

2.2.1. Definition

Trust is a subjective phenomenon which anchors on a number of factors that collectively construct the quality of trustworthiness. Trust, in the primary sense, is a feeling, or an emotion, or an affect. Trusting is a major concern, which is to say not only that it is urgent and important, but also that it is first and foremost a matter of personal responsibility (Flores and Solomon, 1998). Accordingly, trust is largely subject-dependent.

Trust is a trait having congruence between the desired and perceived participation (Driscoll, 1978) and it is characterised by hope, faith, confidence, assurance and initiative (Lewicki et al., 1998). There are two parties, viz. a trustor and a trustee, involved in a trust relationship. The person who trusts someone or something is called a trustor and the one who is being trusted is called a trustee. It is essential that there exists a trusting intention (willingness) as well as trusting belief (belief) between the two parties (McKnight et al., 1998). Additionally, some tact and willingness on the part of the trustor and some willingness on the part of the trustee, both to be forgiven and forgive unfair criticisms, look essential to make the trust relationship successful (Baier, 1986). Trust involves a two-way process which counts both giving and receiving as well.

The sociopsychological account identifies the following characteristics of trust:

- *Trust is asymmetric.*
- *Trust is transitive* (though the level of trust decreases as the links grows longer).
- *Trust is personalised and subjective.*
- *Trust is context-dependent.*

2.2.2. The building blocks

There are two building blocks, namely, cognition and affection, with which trust is being built (McAllister, 1995). Cognition is the learning which is based on perceptual reasoning. Cognitive learning depends on:

- Success of past interactions with the trustee, i.e., past records.
- Extent of social similarity, i.e., the group of friends that the trustee keeps.
- Context considerations, i.e., the credentials owned by the trustee.

Conversely, affection is the gentle feeling of fondness or liking. Affection is based on:

- Nature of the behaviour of the trustee.
- Frequency of interaction between the trustor and the trustee (More the frequency of interaction, higher is the trust. This is because, interaction makes them comfortable in sharing, which in turn, increases the closeness and reliability).

If both cognition and affection are high, the ideal level of trust is available. Generally, cognition is followed by affection, and once affection is high, the foundation of cognition-based trust may not be needed. For instance, people trust others initially in the light of learning through cognition, and once cognition is developed, affection increases with time. Likewise, when affection increases, we overlook the information attained through cognitive learning. Finally, it is to be added that trust is dynamic and continuous variable, because it is dependent on relationships that are ever changing.

2.2.3. Trust model

An in-depth analysis of sociopsychological account unveils that trust is a function of three factors: ability (A), benevolence (B) and integrity (I). The following equation and Fig. 1 (Mayer et al., 1995) elucidate this idea.

$$Trust = f(A, B, I) \tag{1}$$

where:

- *Ability* denotes the capacity of a person in performing a given task. Higher the ability, higher is the trust level. Likewise, lower the ability, lower is the trust level. However, ability is domain specific, and high ability in one task does not guarantee high ability in other tasks.
- *Benevolence* is the stable disposition which capacitates the trustee to do good for the trustor. Effect of benevolence is likely to increase over time as the relationship between the two parties develops.
- *Integrity* is the virtue, which prompts one to act always in accordance with one's own principles. The role of integrity will be more significant in the early stages of relationships. This is