A Trust Model using Fuzzy Logic in Wireless Sensor Network

Tae Kyung Kim, and Hee Suk Seo

***Abstract*—**Adapting various sensor devices to communicate within sensor networks empowers us by providing range of possibilities. The sensors in sensor networks need to know their measurable belief of trust for efficient and safe communication. In this paper, we suggested a trust model using fuzzy logic in sensor network. Trust is an aggregation of consensus given a set of past interaction among sensors. We applied our suggested model to sensor networks in order to show how trust mechanisms are involved in communicating algorithm to choose the proper path from source to destination.

***Keywords*—**Fuzzy, Sensor Networks, Trust.

I. Introduction

WIRELESS sensor network is a wireless network consisting of distributed sensors to deliver real-time data streams for applications such as environmental monitoring, structural engineering and health care etc. A sensor node is a tiny and simple device with limited computation and resources. Sensor nodes are randomly and densely deployed in sensed environment. WSN is designed to detect events or phenomena, collect and send back sensed data to the user. The characteristics of wireless infrastructure and characteristics of WSNs cause the potential risks of attacks on the network. Numerous studies [1] have attempted to address the vulnerabilities in WSNs such as Denial of Service in Sensor Networks [2], Secure Routing in Sensor Networks [3]. Many researches on security related in Wireless sensor network are processed in many fields but it is required to study the mechanisms about distinguishing the wrong sensor among the suitable sensors.

The study on computation model of trust is carried by Marsh [4]. This paper provides a clarification of trust. Also presents a testbed populated by simple trusting agents which substantiates the utility of the formalism. In general, we all make trusting decisions, most of us every day of our lives, and many times per day because trust concerns that which one person can rightly demand of another. We would like to use the reputation of trust to distinguish the suitable sensors and illegal sensors.

This paper introduces an explicit trust to sensors to allow them to reason with and about trust, thereby making them more robust in the face of decision making concerning others. In the next section, we present related work and section III proposes trust model using fuzzy logic for wireless sensor networks. In the section IV, we show the efficiency of suggested model. Finally, the paper ends with a conclusion and future work.

II. Related Works

A. Trust Model

A number of trust algorithms have been proposed. Trust is defined as the extent to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved. A trust decision is binary and based on the balance between trust and risk, and it has some sort of effect on the trustee. Usually it is made with a class of applicable situations in mind, such as concerning a particular trustee in performing a certain action [4].

Early forms of trust management began by automating authentication and authorization decisions with the help of varying sets of credentials. Marsh was one of the first to introduce a computational model for trust in his doctorate thesis [5]. His model is relatively simple, based on a scalar value of trust, and does not discuss reputation. Mayer looked for a differentiation between factors contributing to trust, trust itself and its outcomes [6]. Essin wrote a socio-technologically focused model for trust and policy, with a goal to make them work better in computer systems [7]. Egger [8, 9] has developed a model for trust-relevant factors from a customer's perspective. Some factors are relevant for the perspective of a service provider as well, such as reputation, propensity to trust and transference.

Mathematical models give tools and formulae for dealing with experience as it is represented as a binary for "cooperated vs. defected" [10] or by scalars [11]. The SECURE project provides a formal model of incorporating new evidence to trust information [12, 13]. The Sultan project has also included an experience collection module in its architecture description [14, 15]. Translating experience into updates in reputation seems to largely be work in progress.

There has been some progress in the field of updating trust and reputation based on evidence of the actors' behaviour in the system. Yet while some projects include experience-collection modules in their systems [15, 16], practical studies on how to translate various suspicious or encouraging events into updates of reputation or trust are scarce. Theoretical models considering the topic assume that experiences have already been coded into either binary or scalar [10, 11].

T. K. Kim is with the Seoul Theological University, Bucheon-City, Kyonggi 422-742 Korea (e-mail: tkkim@ stu.ac.kr).

H. S. Seo is with the Korea University of Technology and Education, Byungcheon, Chungnam 330-708 Korea (corresponding author to provide phone: +82-41-1495; fax: +82-41-1462; e-mail: histone@kut.ac.kr).

B. Fuzzy Logic

Fuzzy if-then rules have been applied to many disciplines such as control systems, decision making, pattern recognition and system modeling. The algorithm of fuzzy rule-based inference consists of three steps.

(1) Fuzzy matching: calculate the degree to which the input basic steps and condition of the fuzzy rules.
(2) Inference: calculate the rule's conclusion based on its matching degree
(3) Combination: combine the conclusion inferred by all fuzzy rules into a final conclusion

In [17], they suggested fuzzy model of the sensor that takes in account the sensor uncertainty and they showed a way to make the fusion of fuzzy output data of all sensors taken in a short period of time.

In this paper, we suggested a trust model using fuzzy logic in wireless sensor network to distinguish proper sensor and abnormal sensor. Abnormal sensor can attack and contaminate the wireless sensor network.

III. Trust Model using Fuzzy Logic

A. Wireless Sensor Network

Fig. 1 depicts the architecture of the wireless sensor network.

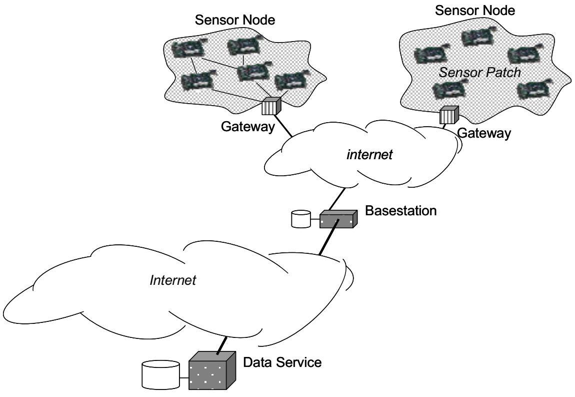

Fig. 1 Wireless Sensor Network

We applied the fuzzy logic in trust model of wireless sensor node.

Stephen Marsh examined the concepts of trust, mistrust, distrust and how they interlink [18]. To use the wireless sensor network in safe state, we should calculate the degree of each sensor node. Then using the information of calculated result, each sensor node decides whether to communicate or not.

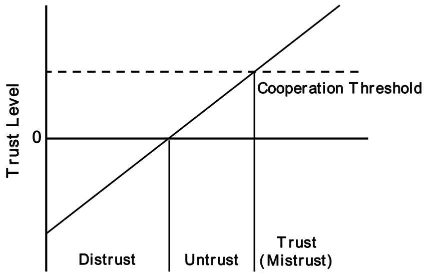

Fig. 2 Concepts of trust, mistrust and distrust

B. Suggested Model

To calculate the trust level of sensor node, we defined T as trustworthiness and U as untrustworthiness. The range of T and U are 0≤ T≤ 1, 0≤ U≤ 1. We assumed that base station in wireless sensor network has the reputation value of each sensor node. Reputation is defined as a perception a party creates through past actions about its intentions and norms [10]. Reputation exists only in a community which is observing its members in one way or another, and is as such meaningless outside its native environment. It can be transmitted from one community context to another [4].

In reputation components, there are a few evaluation value of each sensor node. Then we can define like these:

1. Min: $T = \min(T_i,T_j)$, Min: $U = \min(U_i,U_j)$
2. Max: $T = \max(T_i,T_j)$, Max: $U = \max(U_i,U_j)$

Then we can acquire the trust and untrust value like this:

$$T = \frac{\mathrm{avg}(T_i, T_j)}{1-(avg(T_i, U_j)+avg(T_j, U_i))}$$

$$U = \frac{\mathrm{avg}(U_i, U_j)}{1-(avg(T_i, U_j)+avg(T_j, U_i))}$$

For i and j are included in sensor node sets.

Using the T and U, we can calculate the evaluation level of sensor network.

$$Evaluation\_value = \frac{T}{T+U}$$

The fuzzy trust model provides the dataset shown in Fig. 3.

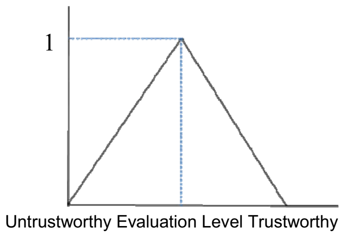

Fig. 3 Fuzzy Output of Trust Model

IV. Performance Evaluations

To show the efficiency of suggested model, we used the scenario based performance evaluation. In this scenario, we recursively applied the suggested numerical formula for two sensor nodes among the paths from S to D and calculate the average value of summing up the result value.

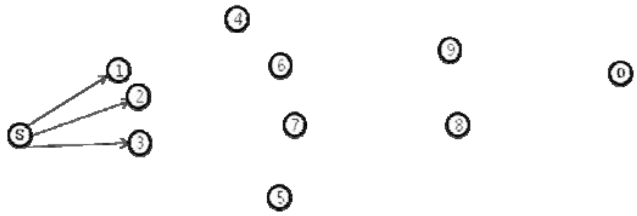

Fig. 4 WSN Architecture

There are many paths from S(Source) to D(Destination). We used the trust model using fuzzy logic to choose the suitable paths from S to D for the purpose of safe communication.

TABLE I
Trustworthy and Untrustworthy of Each Node

sensor node	T	U	sensor node	T	U
S	1.0	0	D	1.0	0
1	0.7	0.2	2	0.5	0.5
3	0.3	0.7	4	0.2	0.8
5	0.3	0.3	7	0.8	0.2
7	0.4	0.3	8	0.1	0.9
9	0.9	0.1			

In the network environment of Fig. 4, we assumed the trustworthy and untrustworthy value of each sensor node like Table I. We randomly choose the path from S to D sensor node using C program and calculate the evaluation value as shown in Table II.

TABLE II
Evaluation Value of Each Path

Path	Evaluation value	
P1: S→ 1→ 7→ 9→ D	S→ 1	0.89437
	1→ 7	0.526316
	7→ 9	0.764706
	9→ D	0.95
P2: S→ 1→ 7→ 8→ D	S→ 1	0.89437
	1→ 7	0.526316
	7→ 8	0.294118
	8→ D	0.55
P3: S→ 2→ 5→ 9→ D	S→ 2	0.75
	2→ 5	0.5
	5→ 9	0.75
	9→ D	0.95
P4: S→ 2→ 7→ 8→ D	S→ 2	0.75
	2→ 7	0.529412
	7→ 8	0.294118
	8→ D	0.55
P5: S→ 3→ 4→ 9→ D	S→ 3	0.65
	3→ 4	0.25
	4→ 9	0.55
	9→ D	0.95

Using the results of Table II, we can calculate the safe and proper path as shown in Fig. 5.

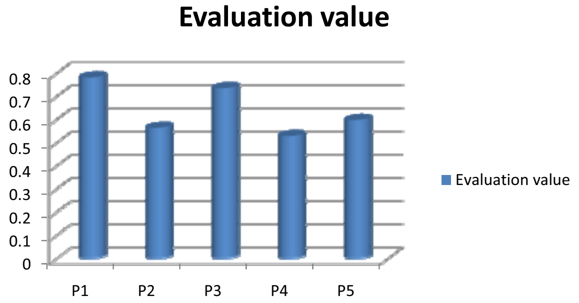

Fig. 5 Trust Evaluation Value of Each Path

We can know that path P1 has high trust value. So if we use the path P1, the packets can be safely transmitted to the destination sensor node without considering the attack of abnormal sensor.

V. Conclusion

In this paper, we formulated the trust model using fuzzy logic for the safe communication between source and destination node in wireless sensor network. We focused on the trustworthy of sensor node which participating the wireless network. If the sensor node has high trust value, other node can trust the sensor node and sending and receiving a data safely with it.

In future, we plan to simulate the suggested model and intend to measure the stability of our model with variation in workload.

References

[1] T. H. Hai, F. Khan, and E. Huh, "Hybrid Intrusion Detection System for Wireless Sensor Networks", ICCSA 2007, LNCS 4706.

[2] Wood, A.D., Stankovic, J.A. "Denial of Service in Sensor Networks", Computer 35(10), 2002.

[3] Karlof, C., Wagner, D. “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Elsevier’s Ad. Hoc. Networks Journal, Special issue on sensor network applications and protocols, 2003.

[4] Sini Ruohomaa and Lea Kutvonen, "Trust Management Survey", iTrust 2005, LNCS 3477, 2005.

[5] Marsh, S., “Formalising Trust as a Computational Concept. PhD thesis”, University of Stirling, Department of Computer Science and Mathematics, 1994.

[6] Mayer, R.C., Davis, J.H., “An integrative model of organizational trust:, The Academy of Management Review 20, 1995.

[7] Essin, D.J., “Patterns of trust and policy”, Proceedings of 1997 New Security Paradigms Workshop, ACM Press 1997.

[8] Egger, F.N., “Trust me, I’m an online vendor: Towards a model of trust for e-Commerce system design”, Conference on Human Factors in Computing Systems, ACM Press, 2000.

[9] Egger, F.N., “From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce”, PhD thesis, Eindhoven University of Technology, 2003.

[10] Mui, L., Mohtashemi, M., Halberstadt, A., “A computational model of trust and reputation”, 35th Annual Hawaii International Conference on System Sciences (HICSS’02). Volume 7., IEEE Computer Society, 2002.

[11] Liu, J., Issarny, V., “Enhanced reputation mechanism for mobile ad hoc networks”, Trust Management: Second International Conference, iTrust 2004, Oxford, UK, March 29–April 1, 2004. Proceedings. Volume LNCS 2995, 2004.

[12] Wagealla, W., Carbone, M., English, C., Terzis, S., Nixon, P., “A formal model on trust lifecycle management”, Workshop on Formal Aspects of Security and Trust (FAST2003) at FM2003. Volume IIT TR-10/2003. IIT-CNR, Italy, 2003.

[13] Cahill, V., et al., “Using trust for secure collaboration in uncertain environments”, Pervasive Computing 2, 2003.

[14] Grandison, T., Sloman, M., “Specifying and analysing trust for Internet applications”, Proceedings of 2nd IFIP Conference on e-Commerce, e-Business, e-Government I3e2002, Lisbon, Portugal, 2002.

[15] Grandison, T.W.A., Sloman, M., “Sultan - a language for trust specification and analysis”, Eighth Workshop of the HP OpenView University Association, Berlin, June 24-27, 2001.

[16] English, C., Terzis, S., Wagealla, W., “Engineering trust based collaborations in a global computing environment”, Trust Management: Second International Conference, iTrust 2004, LNCS 2995, 2004.

[17] Morgado de Gois, J. A., Germann, D., Hiller, M.,"Sensor-based ground detection in unstructured terrain for the walking machine ALDURO", 6th Conference on Climbing and Walking Robots CLAWAR 2003.

[18] Stephen Marsh and Mark R. Dibben, “Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) side”, iTrust 2005, LNCS 3477, 2005.