IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 12, 2017, accepted August 3, 2017, date of publication August 15, 2017, date of current version September 27, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2740219

A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks

ALJAWHARAH ALNASSER[1,2], AND HONGJIAN SUN[2], (Senior Member, IEEE)
[1]Department of Information Technology, King Saud University, Riyadh 11543, Saudi Arabia
[2]School of Engineering and Computing Sciences, Durham University, Durham DH1 3LE, U.K.

Corresponding author: Hongjian Sun (hongjian.sun@durham.ac.uk)

This work was supported in part by the U.K. EPSRC under Grant EP/P005950/1, and in part by the European Commissions Horizon 2020 Framework Programme (H2020/2014-2020), TESTBED Project, under Grant 734325

ABSTRACT Smart grids require communication networks to convey sensing and control data for improving the efficiency of energy generation, transmission, and delivery. As a result, smart girds become vulnerable to various types of cyber-attacks. Trust models were recognized as one of the important methods of defending a large communication network against malicious cyber-attacks. In this paper, a fuzzy logic trust model is proposed to detect untrusted nodes in smart grid networks, and compared with an existing model to show its advantages. Using this proposed model, both the routing efficiency and the detection rate for all types of considered malicious behaviors can be improved. In comparison with the existing lightweight and dependable trust system model, the proposed model improves the packet dropping rate by up to 90% when the percentage of malicious nodes is less than 25%, as verified by simulations.

INDEX TERMS Internet of Things, smart grids, cyber attacks, trust, fuzzy logic, dropping rate.

I. INTRODUCTION

As a result of immense widespread of Internet, a new concept that connects all objects together, known as Internet of Thingsİ (IoT), has emerged. IoT is a new vibrant research field in both computer networks and electronics engineering. IoT transforms the Internet from the interaction between humans only to the interaction between things and humans, and even the interaction between things. This is enabled by giving smart devices the ability of thinking, making decisions without any human intervention, and sharing these information with other smart devices to achieve a specific goal.

A smart grid is one of the typical application environments for applying IoT technologies. Electricity companies launched campaigns for replacing old electricity meters with smart meters that allow two-way communications between smart meters and Metering Data Management System (MDMS) [1]. The meter readings can be directly and automatically sent to MDMS for producing bill etc. without any human intervention. Smart grid communication architecture consists of three layers [2], [3], as shown in Fig. 1: first layer is a Home Area Network (HAN) which consists of all devices within the home or building that is connected with smart meters; second layer is a Neighborhood Area Network (NAN) that is composed of many HANs and a base station (also known as a data concentrator); and third layer is a Wide Area Network (WAN) where base stations forward the concentrated metering data to MDMS.

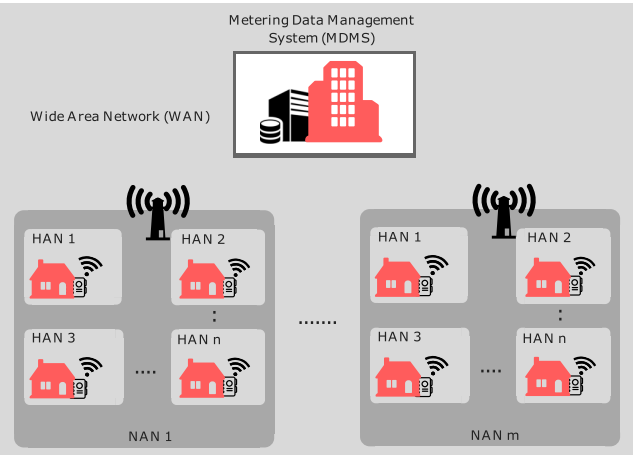

FIGURE 1. Communication infrastructure in smart grid.

In the NAN layer, smart meters create a network to deliver data to the base stations which make them vulnerable to internal or external attacks. Internal attacks are very difficult to detect since the compromised node (smart meter) is considered as an authenticated node. Therefore, applying

This work is licensed under a Creative Commons Attribution 3.0 License. For more information, see http://creativecommons.org/licenses/by/3.0/

traditional security schemes cannot protect the network from these attacks. Hence, there is a need of developing new security methods for dealing with internal attacks. Trust management scheme is one of the most common techniques that were proposed for detecting internal attacks [4], [5]. Each smart meter in the network keeps monitoring its neighbors and reports any misbehaving activity [5]. The compromised node can launch various types of malicious attacks, such as blackhole attack, sinkhole attack, injecting false information and jamming the channels [6]. The smart meters could send the collected data to the data concentrator through the use of a multi-hop routing protocol. As a result, the compromised node can inject itself in the forwarding route and launch attacks to disrupt the routing protocol. For example, the compromised node could stop participating in the packet forwarding process. Indeed, recent works [7], [8] successfully applied trust models to routing protocols in order to forward the data through a secure route by considering the trustworthiness degree for all nodes.

The weighted-sum is one of the most common methodologies that were used for trust management, where trust evaluation can be done by giving different weights for each trust component [9]. Total trust is computed by

$$T_{total} = \sum_{i=1}^{U} w_i \times T_x \tag{1}$$

where w_i is a weight value for T_x which is a trust value for a trust level x such as direct and indirect, and U is the number of trust levels that will be considered. However, this method has the following issues [9]. *First,* setting the optimal weights (w_i) for different trust levels, as shown in equation (1), is very difficult. *Second,* in the existing weighted-sum models, trust levels are typically calculated by using different mathematical schemes and complex models which can cause high resource consumption such as processing power. *Third,* choosing the optimal threshold values is a challenge for this weighted-sum method because the trust decision is made by predefining trust threshold that is typically unknown.

Actually, trust itself is a vague relationship for most instances, and uncertainty is one of its characteristics. It cannot be strictly treated with the likelihood of probability because the probability model contains an evaluation of uncertainty. Even if it becomes feasible, it cannot be generalised for treating all situations. In trust networks, the evidence to be supported may be fuzzy, and the policies to be enforced may be fuzzy too. Thus fuzzy logic, a form of multi-valued logic derived from fuzzy set theory to deal with reasoning [10], becomes a good technical choice. Several fuzzy models were studied to provide a series of fuzzy rules for handling uncertainty situations, which were used in control systems for decision making and pattern recognition. Fuzzy logic incorporates a series of IF-THEN rules to solve a control problem rather than attempt to mathematically model a system. The main steps of fuzzy rule-based inference are as follows [11]:

1) Predefine the fuzzy sets and criteria.
2) Initialize the input variable values to the fuzzy engine, by calculating the degree to which the input basic steps and condition of the fuzzy rules.
3) Apply the fuzzy rules to determine the output data, by calculating the rules conclusion based on its matching degree.
4) Evaluate the results and give certain feedbacks to moderate criteria or rules.

Recently, researchers developed fuzzy logic trust models to build up trust relationships among sensor nodes. For example, in [12], a fuzzy logic trust-based model was proposed. Two sets of parameters were considered as fuzzy inputs. The first set was a node feature such as sensor readings, and battery status. The second set was a link feature such as link quality, received signal strength and packet error rate. However, it did not consider untrusted nodes that can initiate a malicious behavior. Renubala and Dhanalakshmi [13] studied a trust fuzzy logic for enabling secure routing in wireless sensor networks. The model consists of five parameters: reliability, residual energy, buffer occupancy, packet generation rate and speed. The network was protected from the black-hole attack, bad mouthing attack, and contradictory behavior attack. Also, Chen *et al.* [14] studied a trust fuzzy logic model by considering trust evaluation metrics for the establishment and validation of the trust management model: End-to-end Packet Forwarding Ratio (EPFR), Average Energy Consumption (AEC) and Packet Delivery Ratio (PDR). The membership function was created for direct trust and recommendation trust, however, the past trust was computed as a weighted-sum with most recent trust.

In this paper, a new fuzzy logic trust-based model is proposed for a smart grid network for detecting untrusted nodes. The proposed model uses similar mathematical scheme as that was used in a Lightweight and Dependable Trust System (LDTS) model [4]. However, different from [4] that used a fuzzy logic rule to evaluate the trust by maintaining three linguistic input variables (direct, indirect and past trust), we develop an adaptive strategy for trust evaluation. In addition, a comprehensive performance analysis and comparison are performed for analysing weighted-sum method and fuzzy logic method, given similar mathematical scheme adopted in both methods. In brief, the main contributions of this paper are:

1) Different from existing research, this paper first proposes the use of a new fuzzy logic trust model for protecting smart grid networks from cyber-attacks.
2) This paper compares the performance of the proposed model with that of existing weighted-sum trust model, revealing their advantages and disadvantages.
3) A self-adaptive approach for LDTS model is studied for trust evaluation.

The paper is organised as follow. Section II proposes the fuzzy trust model for smart grid networks. Section III illustrates the simulation analysis of the proposed model.

Section IV presents its comparison results with LDTS model. Finally, Section V summarises the overall work performed.

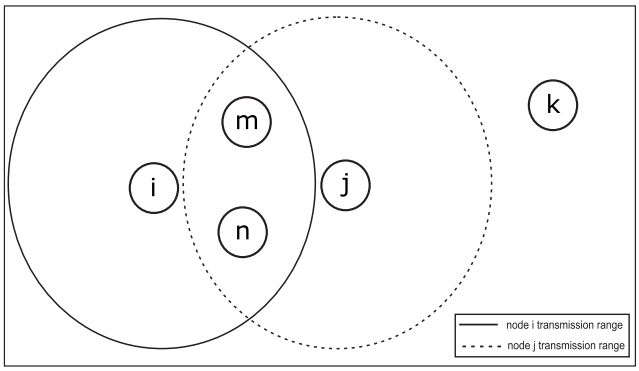

FIGURE 2. Trust evaluation levels.

II. PROPOSED SYSTEM MODEL

A. TRUST DEFINITIONS

Trust measurement is one of the most important schemes to evaluate the trustworthiness between two nodes. Each node monitors its neighbors and computes trust values for them. All nodes in the network applies the trust model as a security tool to continuously monitor their neighbors' behavior. The node that has some misbehaving characteristics can be considered as a compromised node. Using Fig. 2, trust evaluation is done in four levels:

Direct Trust: node i computes direct trust by direct observation of its one-hop neighbors (*node n*, *node m*).

Recommendation Trust: node i computes trust value for two-hops neighbors (*node j*) using the recommendations from the common neighbors (*node m*, *node n*).

Indirect Trust: node i computes trust value for non-neighboring nodes (*node k*) using others nodes recommendations.

Past Trust: each node records the previous trust value of all nodes to keep track of their behavior.

B. THE SYSTEM MODEL

The considered network consists of one NAN. Each NAN has a number of smart meters and one base station used as a collecting node. These smart meters are equipped with a two-way communication between meters and substations which give them the ability to measure and deliver their readings to the collecting node. Smart meters forward the sensed data to the collecting node through the use of multi-hop routing protocol. Because of that, they are assumed to be deployed in a way that ensures the connectivity with one another through a wireless communication.

The network is deployed in urban environment for an electricity monitoring, where each node collects the data and sends them every hour to the collecting node. At the same time, each smart meter continuously monitors its neighbors' behavior and records these information to calculate direct trust. After each sending interval, each node sends its feedback (direct trust) about its neighbors to the collecting node to compute the global trust. If the collecting node detects untrusted node, it isolates it from the network and updates the routing table for each node.

C. PROPOSED TRUST MODEL

The proposed model is a fuzzy logic trust model for achieving a secure routing in the network. It gives the ability for sensor nodes to make a smart decision about the compromised nodes. The proposed model is composed of four steps.

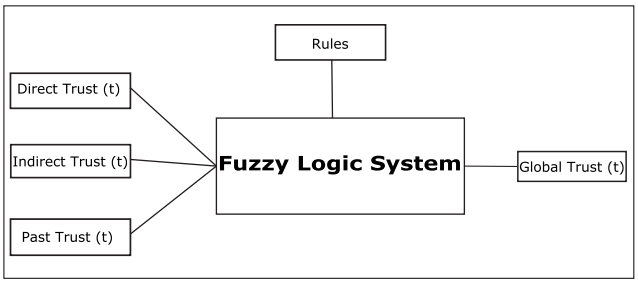

FIGURE 3. Proposed fuzzy logic trust model for secure routing in smart grid networks.

1) LINGUISTIC INPUTS (TRUST COMPONENTS)

as shown in Fig. 3, the model has three inputs which represent trust levels: direct trust, indirect trust and past trust.

a: DIRECT TRUST (SENSOR NODE LEVEL)

As mentioned before, NAN is a multi-hop network where nodes are responsible for forwarding the packets until reach the base station. *Node i* forwards the packets to its neighbor *node j* and keeps monitoring *node j* to verify whether it forwards the packets. The direct trust $DT_{i,j}$ between *node i* and *node j* at time (t) is measured by

$$DT_{i,j}(t) = \frac{forwarded\_Packets}{Total\_Packets} \tag{2}$$

where *forwarded_Packets* is the number of packets that *node j* received from *node i* and forwarded them successfully. *Total_Packets* is the total packets that *node j* received from *node i*.

b: INDIRECT TRUST (BASE STATION LEVEL)

The base station broadcasts a request periodically to collect the direct trust from all nodes in the network. Indirect trust is a centralized operation where the base station computes the indirect trust between the base station and each node in the network based on nodes' feedback [4]. The base station fills the matrix with the nodes' feedback using

$$Feedback = \begin{bmatrix} DT_{1,1} & \dots & \dots & DT_{1,n} \\ \vdots & \dots & \dots & \vdots \\ \vdots & \dots & \dots & \vdots \\ DT_{n,1} & \dots & \dots & DT_{n,n} \end{bmatrix} \tag{3}$$

where n is the number of sensor nodes in the network. Indirect trust $ID_{BS,i}$ between base station and *node i* at time (t) is computed using

$$ID_{BS,i}(t) = \frac{\sum_{k=1}^{m}(DT_{k,i})}{m} \tag{4}$$

where m is the number of nodes that have a feedback about *node i*, $m \leq n$.

c: PAST TRUST

The model should keep track of the historical behavior of each node because that could affect the network performance. Smart compromised nodes could behave as a normal and malicious alternatively to escape from the punishment. The past trust T_{Past} at time (t) is computed using the following equation:

$$T_{Past}(t) = \frac{\sum_{i=1}^{t-1} GT(i)}{t-1} \tag{5}$$

where GT(i) is the global trust that will be defined in step 4.

2) FUZZIFICATION PROCESS

the input linguistic variables are connected through AND logical operator. The proposed model uses a triangular and trapezoidal membership functions to map crisp (input) values to fuzzy sets. The fuzzy numbers H, A, and L denote High, Average and Low respectively.

First, the membership function of the fuzzy number H is defined as

$$M_H(x) = \begin{cases} 0, & x < a_1 \\ \dfrac{x-a_1}{a_2-a_1}, & a_1 \leq x \leq a_2 \\ 1, & x > a_2 \end{cases} \tag{6}$$

Next, the membership function of the fuzzy number A is computed as

$$M_A(x) = \begin{cases} 0, & x \leq b_1 \\ \dfrac{x-b_1}{b_2-b_1}, & b_1 < x \leq b_2 \\ \dfrac{b_3-x}{b_3-b_2}, & b_2 < x < b_3 \\ 0, & x \geq b_3 \end{cases} \tag{7}$$

Finally, the membership function of the fuzzy number L is derived by

$$M_L(x) = \begin{cases} 0, & x > c_1 \\ \dfrac{c_1-x}{c_1-c_2}, & c_2 \leq x \leq c_1 \\ 1, & x < c_2 \end{cases} \tag{8}$$

TABLE 1. Regions boundaries.

Input	a_1	a_2	b_1	b_2	b_3	c_1	c_2
Direct	0.6	0.8	0.1	0.5	0.8	0.5	0.1
Indirect	0.5	0.8	0.1	0.4	0.8	0.5	0.1
Past	0.6	0.8	0.1	0.5	0.8	0.5	0.1

These functions are used because they are computationally efficient to be applied in sensor nodes. The region boundaries is changed in direct, indirect and past trust inputs. Table 1 presents the region boundaries of each input.

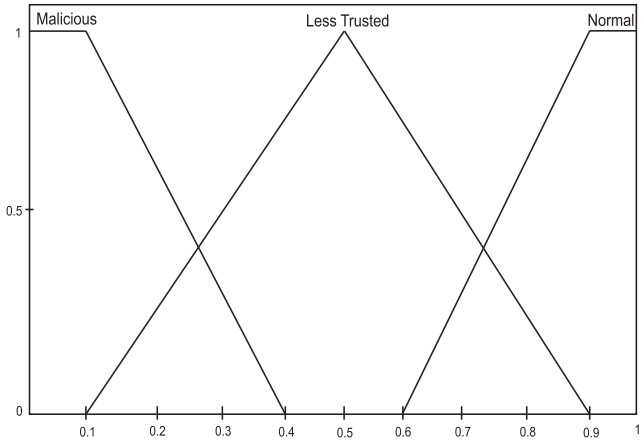

FIGURE 4. Membership functions for global trust.

3) FUZZY INTERFERENCE RULE-BASE

trust values are calculated by passing the fuzzy sets described above through fuzzy inference rules. As shown in Fig. 4, Global Trust (GT) uses Triangular and Trapezoidal Membership Functions which are specified by three parameters: Malicious, Less Trusted, Normal. The formal syntax of the first rule in the rule-base, as an illustration, is given by

IF **Direct** *is* **Low** *AND* **Indirect** *is* **Low** *and* **Past** *is* **Low** *then* **GlobalTrust** *is* **Malicious**. (9)

The number of the input linguistic variables is three in the proposed method and each variable takes three values. Thus, the total number of rules, with all possible combinations, is 27.

4) DEFUZZIFICATION (GLOBAL TRUST - $GT(t)$)

after fuzzification, the next step is a defuzzification to get crisp values using mathematical method. Middle of Maximum (MoM) method of defuzzification is used, which is an efficient method for the resource-constraint sensor nodes [15]. The function gets the middle value of the maximum range of rules aggregation.

III. SIMULATION ANALYSIS

A. SIMULATION SETUP

In our simulations, we considered a network with 16 smart meters and one base station with parameters as shown

FIGURE 5. Network model.

TABLE 2. Simulation parameters.

Parameters	Value
Simulation time ($rounds$)	40
Transmission range (m)	149
Number of sensor nodes	16
Number of malicious nodes	1-4
Simulation area (m^2)	300x500
Trust intervals	10

in Table 2. The meters were randomly distributed over an area of $300 \times 500\ m^2$ with static locations where *node* 3 is the base station (Red node in Fig. 5). All smart meters assumed to have the same resources.

The attacker tried to compromise a node that located in hotspot area of the base station. Then, compromised node can initiate two types of malicious behaviors:

1) TRUST ATTACKS

these attacks infect the trust model itself and make it unable to detect the compromised nodes. The compromised node always tries to gain high reputation using non-stable malicious behavior such as:

a: CONTRADICTORY BEHAVIOR ATTACK

malicious node behaves normally with a group of neighboring nodes and behaves maliciously with the others [16].

b: ON-OFF ATTACK

malicious node behaves normally and maliciously alternately with time. Indeed, it behaves normally during a specific time interval (t) and behaves maliciously during the next time interval ($t+1$) [17].

2) ROUTING ATTACKS

the aim of these attacks is disrupting the multi-hop routing protocols.

Blackhole attack is the most common routing attacks where the malicious node drops all received packets. It causes partition the network where some important information does not reach the base station. Also, it decreases the network performance and increases the end-to-end delay [18].

To measure the performance of our model, we assumed that *node* 4 is a compromised node that initiate a blackhole attack. It drops all received packets from its neighbors (*node* 1, *node* 6, and *node* 10). In addition to blackhole attack, the *compromised node* 4 launches trust attacks to conceal itself by performing non-stable malicious behavior.

B. RESULTS

1) DETECTION OF CONTRADICTORY BEHAVIOR ATTACK

this attack is difficult to detect because of the various feedback from neighbors of the malicious node. Indeed, *compromised node* 4 behaves maliciously with *node* 10 by dropping all packets that received from that node, and behaves normally with others (*node* 1 and *node* 6). In this situation, *node* 1 and *node* 6 will give positive feedback about *compromised node* 4, while *node* 10 has a negative feedback.

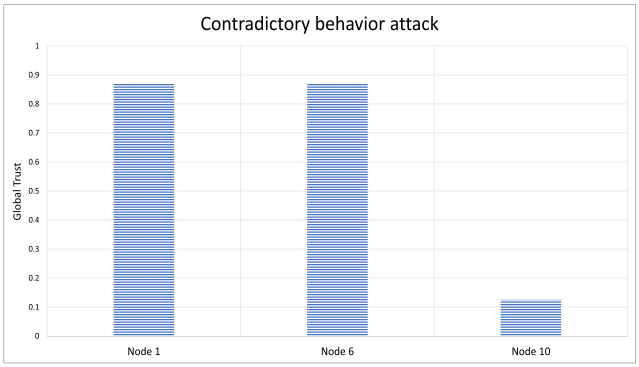

FIGURE 6. Detection of contradictory behavior attack in the proposed model.

Our proposed model gives a high priority for direct trust which is more accurate because it is based on direct experience without any external influences. The corresponding result is shown in Fig. 6. The following remarks can be made:

- *node* 6 and *node* 10 consider *node* 4 as a normal node, because the monitoring result concluded that all packets are forwarded by *node* 4;
- *node* 10 (*victim node*) can detect *malicious node* 4 and change the route to one that is more trusted.

2) DETECTION OF ON-OFF ATTACK

direct trust value reflects the most recent status of a nodes behavior which gives the opportunity for smart attackers to initiate on-off attack [17]. Because of the limitation of node's resources, some trust schemes disregard past interaction experience in trust measurement.

In this case, we assumed that *compromised node* 4 initiate blackhole attack with all nodes in *round* (n), while it behaves normally in *round* ($n+1$). By inspecting Fig. 7, the following remarks can be made:

- in *round* (n), the malicious node can be detected by its neighbors because the malicious activity is targeted all neighbors;

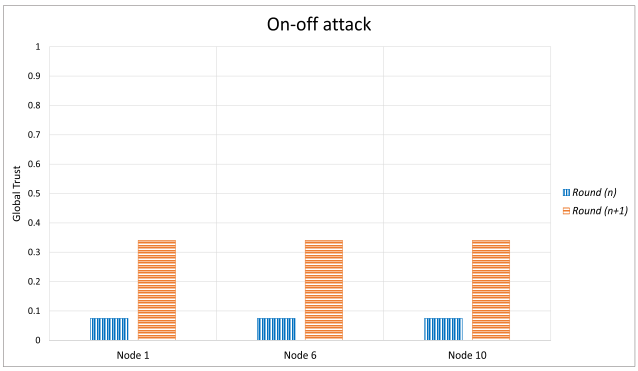

FIGURE 7. Detection of on-off attack in the proposed model.

- in *round* $(n+1)$, global trust for the compromised node increases because of its good behavior. However, it is still considered a malicious node because of its past activities. Thus, the proposed model can reduce the impact of on-off attack.

3) DETECTION OF BLACKHOLE ATTACK

blackhole attacks violate the availability requirement where the malicious nodes stop forwarding the packets that they received from reaching the destination [18]. It reduces the network performance; therefore, we implemented our model in the routing protocol to detect and revoke the compromised node from the routing tables. Each node chooses the next hop based on the trust value; as a result, the packet will be forwarded through a trusted path.

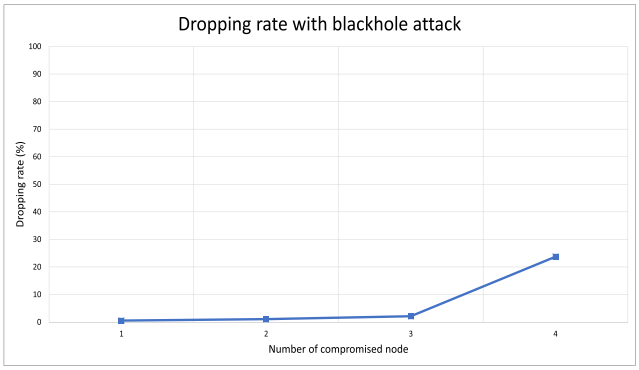

FIGURE 8. Dropping rate in the proposed model.

To measure the performance of our model, we run the simulation many times with a different number of malicious nodes. We assume a stable behavior of compromised node for the whole time by dropping all nodes that received from all neighbors. The result that is shown in Fig. 8 represents the dropping rate during 10 trust intervals. The following remarks can be made:

- in general, the dropping rate increases, as long as, the number of malicious nodes increases;
- if the percentage of malicious nodes is less than 25%, the dropping rate is very small;
- if the percentage of malicious nodes equals to 25%, the dropping rate increases to reach 24%.

IV. PERFORMANCE EVALUATION

We use LDTS model [4] as a benchmark to evaluate the performance of the proposed model.

A. MEASURES DEFINITION

LDTS model used various ways to compute global trust at different levels, we focus on CH level where each CH measures the direct trust and indirect trust then uses the weighted-sum method to compute the global trust $O_{i,j}(\Delta t)$ using the following equations:

$$O_{i,j}(\Delta t) = \lceil 10 \times (w_1 \times \mathcal{C}_{i,j}(\Delta t) + w_2 \times \mathcal{F}_{i,j}(\Delta t)) \rceil \quad (10)$$

$$w_1 = \frac{\Phi(S)}{\Phi(S) + \Phi(g)}, \quad w_2 = \frac{\Phi(g)}{\Phi(g) + \Phi(S)} \quad (11)$$

$$\Phi(x) = 1 - \frac{1}{\alpha + x} \quad (12)$$

where $\mathcal{C}_{i,j}(\Delta t)$ is a direct trust, $\mathcal{F}_{i,j}(\Delta t)$ is indirect trust. S is the number of successful interactions of *node i* with *node j* during Δt, and g is the amount of positive feedback about *node i*. w_1 and w_2 are direct and indirect weighs respectively.

B. CASE STUDY 1: PERFORMANCE COMPARISON FOR TRUST ATTACKS

The aim of trust attacks is concealing malicious nodes from the security model by performing a non-stable malicious behavior. Considering non-stable behaviors is very important while designing trust model, because they can be non-visible to trust model. They allow for the compromised node to stay longer time and destroy the network. Therefore, we compared the results of both models in case of trust attacks.

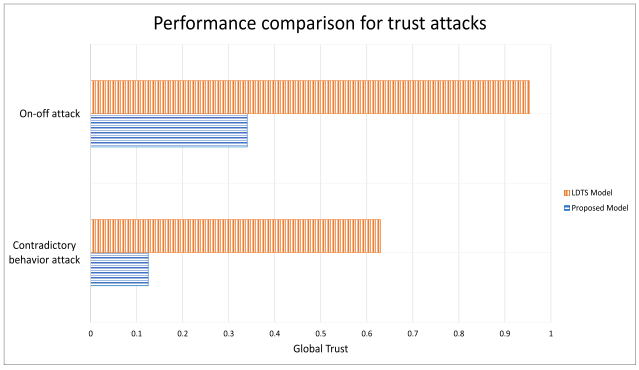

FIGURE 9. Comparison the detection of trust attacks in LDTS and the proposed model.

1) CONTRADICTORY BEHAVIOR ATTACK

as shown in Fig. 9, the attack is detected more easily by our model compared with LDTS model. Because in LDTS, the *victim node* 10 considered the indirect trust only by giving the priority to the nodes' feedback and disregarding its

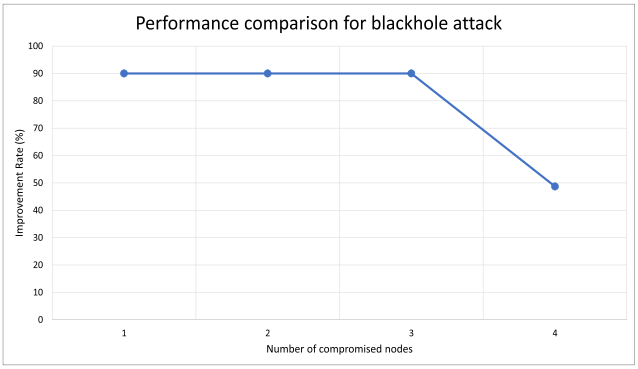

FIGURE 10. Improvement rate in dropping rate in the proposed model.

own experience. The following points present the proof of LDTS result.

- successful interactions between *victim node* 10 and *malicious node* 4 is equal to zero (S = 0), where *malicious node* 4 drops all packets that are received from *node* 10;
- the number of positive feedback about *malicious node* 4 is equal to two [from *node* 1 and *node* 6];
- in this case, the total trust only considers indirect trust, because the weights are as follow $[w_1 = 0, w_2 = 1]$, based on their assumption $\alpha = 1$.

Proof:

$$S = 0, \quad g = 2,$$
$$\Phi(S) = 1 - \frac{1}{1+0} = 1 - 1 = 0$$
$$\Phi(g) = 1 - \frac{1}{1+2} = 1 - 0.33 = 0.67$$
$$w_1 = \frac{0}{0+0.67} = 0$$
$$w_2 = \frac{0.67}{0+0.67} = 1$$

Based on predefined trust threshold ($T_{th} = 0.5$) used in [4], *node* 10 always considers *node* 4 as a normal node.

2) ON-OFF ATTACK

the result in Fig. 9 shows the trust value for the compromised node when it behaves normally in round $(n + 1)$. From the result we can conclude the following:

- in the proposed model, the node is considered as malicious node;
- in LDTS model, the node is considered as a fully trusted node because LDTS scheme only considers past behavior during a specific period of time (n) and (n + 1) separately. Therefore, if the compromised node behaves maliciously during time interval (n), the trust value is low during this interval. Thereafter, if the compromised node behaves normally in the next time interval $(n + 1)$, the trust value increases during this interval and disregards the malicious behavior in previous rounds.

C. CASE STUDY 2: PERFORMANCE COMPARISON FOR BLACKHOLE ATTACK

In comparison with LDTS model, we measure the improvement percentage of dropping rate in case of stable blackhole attack. From the result in Fig.10, we can concluded the following:

- dropping rate in our model is improved by 90% while the number of malicious nodes is less than 25% of network nodes;
- When the number of malicious nodes is equal to 25%, the improvement is decreased to reach 58%.

V. CONCLUSION

In this paper, we presented a fuzzy logic trust model to detect malicious nodes that stop forwarding packets. Also, we considered non-stable behaviors that affect trust model such as contradictory behavior attack and on-off attack. We compared this proposed trust model with existing trust scheme LDTS which used weighted-sum model. Simulation results showed that our proposed model outperforms LDTS trust model. We concluded that our proposed model can improve the detection rate and the network efficiency with lower dropping rate. A comparison of the proposed model with the LDTS model showed its superiority and adaptation of detection with almost all types of nodes. The network performance was improved by 90% while the number of malicious nodes is less than 25%. Thus, it gives network designers a full package that delivers trustworthy messages through a safe path with high reliability.

VI. FUTURE WORK

In future work, we will apply the proposed model in real MICAz sensor motes and compare these practical results with our simulation results. We could also combine the proposed trust model with the routing protocol such as (AODV). The proposed model could be applied to different IoT applications such as Vehicular Ad-hoc Network (VANET) with mobility factor.

REFERENCES

[1] J. Jiang and Y. Qian, "Distributed communication architecture for smart grid applications," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 60–67, Dec. 2016.
[2] J. Jiang and H. Sun, "Performance assessment of distributed communication architectures in smart grid," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.
[3] Y. Zhang, L. Wang, and W. Sun, "Trust system design optimization in smart grid network infrastructure," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 184–195, Mar. 2013.
[4] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.
[5] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.
[6] Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proc. INFOCOM Conf.*, 2006, pp. 1–13.
[7] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET Inf. Security*, vol. 6, no. 2, pp. 77–83, Jun. 2012.

[8] M. Xiang, W. Liu, and Q. Bai, "Trust-based geographical routing for smart grid communication networks," in *Proc. 3rd IEEE Int. Conf. Smart Grid Commun.*, Nov. 2012, pp. 704–709.
[9] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "TERP: A trust and energy aware routing protocol for wireless sensor network," *IEEE Sensors J.*, vol. 15, no. 12, pp. 6962–6972, Dec. 2015.
[10] N. Sirisala and C. S. Bindu, "Uncertain rule based fuzzy logic QoS trust model in manets," in *Proc. Int. Conf. Adv. Comput. Commun. (ADCOM)*, 2015, pp. 55–60.
[11] C. Wagner, A. Pourabdollah, M. Smith, and K. Wallace, "Capturing subjective relationships between variables from human experts," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2015, pp. 2033–2038.
[12] M. Usman, V. Muthukkumarasamy, and X.-W. Wu, "Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 197–205, Feb. 2015.
[13] S. Renubala and K. Dhanalakshmi, "Trust based secure routing protocol using fuzzy logic in wireless sensor networks," in *Proc. Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, 2014, pp. 1–5.
[14] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things," *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.
[15] X. Liu, "Parameterized defuzzification with maximum entropy weighting function—Another view of the weighting function expectation method," *Math. Comput. Model.*, vol. 45, no. 1, pp. 177–188, 2007.
[16] R. Deshmukh, R. Deshmukh, and M. Sharma, "Rule-based and cluster-based intrusion detection technique for wireless sensor network," *Int. J. Comput. Sci. Mobile Comput.*, vol. 2, no. 6, pp. 1–9, 2013.
[17] N. Labraoui, "A reliable trust management scheme in wireless sensor networks," in *Proc. 12th Int. Symp. Programm. Syst. (ISPS)*, 2015, pp. 1–6.
[18] M. Wazid, A. Katal, R. S. Sachan, R. Goudar, and D. Singh, "Detection and prevention mechanism for blackhole attack in wireless sensor network," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, 2013, pp. 576–581.

ALJAWHARAH ALNASSER received the M.Sc. degree in computer engineering from King Saud University, Saudi Arabia, in 2015. She is currently pursuing the Ph.D. degree in computing sciences with Durham University, U.K. Since 2011, she has been a Lecturer with the Department of Information Technology, King Saud University. Her research interests focus on trust management in Internet of Things, wireless communications, and network security.

HONGJIAN SUN (S'07–M'11–SM'15) received the Ph.D. degree from the University of Edinburgh, U.K., in 2011. He holds post-doctoral positions with King's College London, U.K., and Princeton University, USA. Since 2013, he has been with the University of Durham, U.K., as a Lecturer and then a Reader in Smart Grid. He has authored or co-authored over 80 papers in refereed journals and international conferences. He has made contributions to and co-authored the IEEE 1900.6a-2014 Standard. He has authored or co-authored five book chapters, and edited two books: IET book *Smarter Energy: From Smart Metering to the Smart Grid*, and CRC Book *From Internet of Things to Smart Cities: Enabling Technologies*. His research mainly focuses on: 1) smart grid: communications and networking; 2) smart grid: demand side management and demand response; and 3) smart grid: renewable energy sources integration.

He is on the Editorial Board of the *Journal of Communications and Networks*, and *EURASIP Journal on Wireless Communications and Networking*. He also served as a Guest Editor of the *IEEE Communication Magazine* for two feature topics, including: Integrated Communications, Control, and Computing Technologies for Enabling Autonomous Smart Grid, 2016.