IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON TRUSTED COMPUTING

Received September 13, 2018, accepted October 21, 2018, date of publication November 2, 2018,
date of current version December 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2879360

A Dynamic Behavior Monitoring Game-Based Trust Evaluation Scheme for Clustering in Wireless Sensor Networks

LIU YANG[1], YINZHI LU[2], SHENG LIU[3], TAN GUO[1], AND ZHIFANG LIANG[1]

[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]School of Electronic Information Engineering, Yangtze Normal University, Chongqing 408100, China
[3]School of Data Science, Tongren University, Tongren 554300, China

Corresponding author: Liu Yang (yangliu@cqupt.edu.cn) and Yinzhi Lu (henanluyinzhi@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61801072, in part by the Chongqing Science and Technology Commission under Grant cstc2018jcyjAX0344, and in part by the Department of Science and Technology of Guizhou Province under Grant LH[2017]7320 and Grant LH[2017]7321.

ABSTRACT A typical wireless sensor network (WSN) is often deployed in harsh or hostile environment to work in an unattended mode. It is prone to various attacks during routing process as the open wireless medium. Traditional encryption and authentication-based secure mechanisms cannot avoid the attacks from internal compromised nodes, and they also need much resource for complex computing. To conquer these problems, trust-based secure mechanism is usually used in WSNs. However, how to get the behavior evidences for trust assessment is rarely addressed to date. In this paper, we present a game theory-based dynamic behavior monitoring scheme for evidences collection in WSNs. A tradeoff between network security and energy conservation can be achieved. Based on this behavior monitoring scheme, a trust assessment mechanism is proposed, which is further integrated into cluster-based routing protocol. Simulation results show that our trust evaluation scheme can gain a higher network lifetime than full-time behavior monitoring-based trust evaluation scheme, while the performance of network security is not degraded.

INDEX TERMS Behavior monitoring, game theory, network lifetime, security, trust, wireless sensor networks (WSNs).

I. INTRODUCTION

Recent advances in Internet of Things (IoT) have greatly promoted the development of Wireless Sensor Networks (WSNs) since they are the perceptual layer of the whole system [1]. A typical Wireless Sensor Network (WSN) is composed of large numbers of sensor nodes with sensing, processing and communication abilities [2]. After deployed into the sensor field, these nodes can automatically self-organize into an ad hoc network. Wireless Sensor Networks (WSNs) have been widely applied in many domains for monitoring and surveillance purposes, it is difficult to recharge or replace the battery for sensor nodes as the unattended working mode and harsh or hostile environment [3]. Wireless transmission usually consumes the majority energy resource of the network [4], hence an energy-efficient routing scheme is essential for enhancing the network lifetime. And the open working environment may lead to variety of attacks during data transmission [5], such as false routing information, selective forwarding, black hole attack, sybil attack and wormhole attack. These attacks may cause improper transmission through forging, falsifying, dropping the data or tempering with the key routing address. Therefore, it is important to integrate the security mechanism into the routing protocol to assure data honesty, integrity and validity.

Traditional encryption and authentication based secure mechanisms are not suitable for WSNs due to their own characteristics [6]. Firstly, sensor nodes have limited energy resource that restricts their communication and computing abilities. And then, network topology frequently changes due to external or human factors. At last, sensor nodes deployed in the hostile environment are easily trapped to become internal malicious nodes with legal identities. Hence, designing a proper secure routing protocol for WSNs is with great challenges as these issues must be concerned. In recent years, the concept of trust is introduced into WSNs to give new insights for solving secure routing problem [7]–[9].

Each node in the network is labeled with a trust degree that representing its reliability. The trust degree of a node is usually evaluated by its neighbor nodes based on the past monitored behaviors. If a collaborative behavior is monitored, the trust degree of this node can be updated. Otherwise, a decline in trust degree may occur.

For trust evaluation in WSNs, a sensor node should keep active to monitor the behaviors of its next hop node after transmitted the data packet [10]. During the data transmission process, packet latency, loss, collision or retransmission may occur as the instability of wireless medium [11]. Thus, the monitoring node should stay in active state for a long duration at times to ensure the behaviors of the monitored node can be captured. The behavior monitoring with longer duration needs more energy consumption, but this operation can improve the security level of the network simultaneously [12]. As the rareness of energy resource in WSNs, an energy-efficient behavior monitoring scheme is necessary for prolonging network lifetime. However, how to design this monitoring scheme for WSNs is rarely addressed to date. Since cluster based network model is more efficient than flat model [13], in this paper we will devote to design a dynamic behavior monitoring scheme for trust evaluation in clustered WSNs. Since game theory is an effective mathematical method that can be used for rational individuals to make decisions under conflict situation [12], it will be used to find an equilibrium solution between network security and energy reservation in our designed scheme. The main contributions of our work are listed as follows:

- We present a dynamic behavior monitoring scheme to collect behavior evidences for trust evaluation in clustered WSNs, where game theory is introduced to achieve a balance between energy consumption and network security.
- The rationality and selfishness factors are integrated into our dynamic behavior monitoring scheme, where malicious behavior value is predicted by the monitoring node when it makes decisions about the monitoring duration. The expected trust value is evaluated by each malicious node to decide whether to take a cooperative action.
- The randomness of wireless channel quality and node failure or misbehavior is considered in our behavior monitoring scheme, so that the fuzziness of behavior evidences can be decreased effectively.
- Based on our behavior monitoring scheme, we present a trust evaluation mechanism, where the evidences from the behavior monitoring are used as the assessment basis.
- Our trust evaluation mechanism is introduced into cluster based routing protocol to evaluate the performance of the trust evaluation mechanism from the aspects of network lifetime and successful forwarding rate of data packets.

The rest of this paper is organized as follows: After the related works are summarized in Section II, system model is presented in Section III. In Section IV, we present our dynamic behavior monitoring game. Based on this game, we propose a trust evaluation scheme which is further integrated into clustering protocol in Section V. We evaluate the performance of our trust evaluation scheme in Section VI. And finally, we conclude this paper in Section VII.

II. RELATED WORKS

Recent years, trust based secure mechanisms for WSNs have attracted the attention of numerous scholars. A secure and accurate data fusion method for WSNs is addressed in [14], where a data fusion model called Double Cluster Heads Model (DCHM) is presented by combining clustering protocol, reputation and trust systems, and data fusion algorithms. The framework of DCHM is composed of Cluster Module, Cluster Head (CH) Module and Base Station (BS) Module. Cluster Module includes Clustering, Cluster Heads (CHs) Election, Reputation and Trust System Construction or Update. CH Module includes Weighted Outliers Detection, Credible Data Fusion, Fusion Results and Outliers Uploading. Based on the reputation and trust system, two CHs are selected in each cluster after clustering, and they perform outlier detection, data fusion and results uploading to BS independently. The dissimilarity coefficient of the two data fusion results are computed at the BS. Based on the dissimilarity coefficient and the lists of outliers, a feedback is sent to the Cluster Module helps to update reputation and trust system. This paper only gives the trust based secure framework, but how to evaluate the trust level for sensor nodes is not descripted in detail.

Sensor nodes usually are responsible to monitor the behaviors of the neighbor nodes in trusted WSNs. And then the supervised results are used as the evidences of trust reputation. In [15], the trust value of sensor nodes is computed by combing direct and recommended trust evidences. As a bigger number of trust replies from neighbors may cause unnecessary overheads, and a smaller number of replies may reduce the network security level. Then a Dilemma Game in Trust Derivation is introduced, where each game participating node decides whether reply the trust request from the evaluating node to achieve a tradeoff between network security and energy efficiency.

Because of the uncertainty property of trust relationship between sensor nodes, such as fuzziness and randomness, the accuracy of trust metric is low in most existing trust management method. To address this problem, a cloud model based trust evaluation method for clustered WSNs is proposed in [16]. Firstly, trust expectations including communication factor, message factor and energy factor will be calculated. After a period of expectations collecting, these sample values serve as cloud drops to construct absolute trust cloud for each factor. To make trust value correspond with standard grade trust cloud and meet security requirements, each absolute factor trust cloud is transformed into relative trust cloud. Secondly, adjustable weights are designed for each factor trust cloud, and immediate trust cloud is obtained by combining these clouds. Thirdly, immediate trust cloud

and recommendation trust cloud are synthesized according to time sensitive factor to get the final trust cloud. Finally, the final trust cloud of sensor node is converted to trust grade by comparing similarity between final trust cloud and five standard grade trust clouds. This paper gives a detail of the trust evaluation method, but how to get the evaluation evidences is not addressed.

A security mechanism for cluster-based WSNs against selective forwarding is proposed in [17]. Sensor nodes in the network are grouped into several clusters, and each one consists of one CH, Inspector Node (IN) and some Member Nodes (MNs). IN monitors CH's data forwarding behavior for attack detection, and its monitoring records will be randomly checked by CH for working supervision. The results from the CH and IN will be ascertained by MNs based on their own evaluation mechanism. To take both the security and lifetime of the network into consideration, the Composite Reputation Value (CRV) that contains forwarding rate and residual energy of the node is utilized to choose the CH and IN under a novel multi-hop cluster based network arrangement, where node density of the cluster is inversely proportional to the distance to BS for energy balance. Simulation results show that this proposed protocol has lower false alarm rate than Watchdog, and longer network lifetime than LEACH.

Considering the open working environment and limited energy resource of the network, a mixed and continuous monitor-forward game is constructed to mitigate the selective-forwarding attack in [12]. The suspicious node in the game plays a mixed strategy to decide whether forwarding packets for other nodes, and the monitoring node plays a continuous strategy to determine the duration of behavior surveillance. The game ends at the equilibrium point where a tradeoff between energy conservation and network security can be achieved. However, this mixed and continuous monitor-forward game does not well take into account of the actual conditions. On the one side, the selfishness and rationality of sensor nodes are not thoroughly considered. On the other side, the randomness of wireless medium quality and node failure or misbehavior is not modeled in the game.

III. SYSTEM MODEL

A. NETWORK MODEL

Hierarchical network model will be used in this paper that all sensor nodes in the network are grouped into clusters [18], and each cluster includes one CH node and several normal MNs. Each normal node decides whether join a cluster according to the distance to the corresponding CH and the evaluated trust value. Then it transmits the data to the CH and monitors the followed behaviors of this CH based on its own interests. Each normal CH aggregates MNs' data and forwards the data to BS. And the malicious CH decides whether cooperatively forwarding the data from MNs according to its own expected trust level.

B. SECURITY MODEL

In this paper, we study how to use game theory to solve the behavior evidence collection problem in trusted WSNs. To construct the security model [19] realistically, we assume all sensor nodes are rational and selfish enough to compete for their own interests under the hostile environment where malicious nodes exist. Each normal node needs to monitor the behaviors of other nodes for trust evaluation, but the longer duration of behavior monitoring causes more energy consumption. And each malicious node expects to enhance its trust level for initiating attacks more conveniently. Moreover, malicious nodes do not worry much about their occasional malicious behaviors as the existence of instable wireless medium and random node failure or misbehavior. If a malicious behavior is captured by a node, this node cannot consider whether the monitored node is malicious or not except reducing the corresponding trust level.

C. RADIO MODEL

During the data transmission process, the amount of energy spent by a sensor node for a k-bit packet with distance d can be calculated as follows [20]:

$$E_{Tx}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, & d < d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4, & d \geq d_0 \end{cases} \quad (1)$$

Where E_{elec} is the amount of energy spent by transmitter or receiver circuitry; ε_{fs} and ε_{amp} are amplifier characteristic constants with regard to free-space propagation model and two-ray ground reflection model respectively; d_0 is the distance threshold used to distinguish the two path loss models, and we can calculate it as follows [21]:

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{amp}} \quad (2)$$

The amount of energy consumed by the receiver can be expressed as follows [22]:

$$E_{Rx}(k) = kE_{elec} + kE_{DA} \quad (3)$$

Where k is the length of received packet; E_{DA} is the amount of energy consumed to aggregate a one-bit packet.

IV. DYNAMIC BEHAVIOR MONITORING GAME

A. GAME OPERATION

In this section, we will introduce a dynamic behavior monitoring game played by a node to decide the duration of behavior monitoring after a data packet is transmitted. We formally define it as $BMG = \{N, S, U\}$, where N is the set of players consisting of monitoring node N_{ing} and monitored node N_{ed}, $S = \{S_i | i \in N\}$ is the strategy combination of all players and $U = \{U_i | i \in N\}$ is the utility function combination. For the monitoring node N_{ing}, its strategy set is $S_{ing} = \{hT | 0 \leq h \leq H\}$, where T is the average round-trip time of one-hop data transmission, h is the multiple of T and H is the upper limit of h. For the monitored node N_{ed}, assuming it adopts the mixed strategy $S_{ed} = \{p, 1-p\}$, where p is the probability of cooperative behaviors.

TABLE 1. Payoff Matrix of the Gam.

	$N_{ed}.c$	$N_{ed}.nc$
$N_{ing}.h$	$-hE_m+E_c$, $-E_c+hE_m$	$-hE_m+A_sCh/H$, $-Ph/(V_sH)+hE_m$

In the behavior monitoring game, each player is a rational and selfish individual that always expects to improve its own payoff. However, the payoff of a player is not only related to its own strategy, but also subject to the strategy combination of all other players [23]. The payoff matrix of this game is shown in Table 1, where $N_{ing}.h$ is the strategy of node N_{ing} to monitor the behavior of node N_{ed} for a duration hT; $N_{ed}.c$ is the strategy of node N_{ed} to conduct a cooperative action; $N_{ed}.nc$ is the strategy of node N_{ed} to conduct a no-cooperative action; E_m is the amount of energy consumed by N_{ing} to take the monitoring action for a duration T; E_c is the amount of energy consumed by N_{ed} to conduct a cooperative action; A_s is the own expected trust value of N_{ed}; V_s is the malicious behavior value of N_{ing} which is predicted by N_{ed}; C is the award to N_{ing} when a malicious behavior is captured and P is the punishment to N_{ed} for its malicious behavior.

Table 1 shows that when N_{ed} conducts the non-cooperative action, N_{ing} can gain more if it executes a longer duration of monitoring. Correspondingly, the punishment inflicted on N_{ed} will be heavier. If N_{ed} expects a higher trust value, N_{ing} will be easily attracted to execute a monitoring action for more awards. A higher predicted malicious behavior value will lead to a slighter punishment to N_{ed}. This is because sudden malicious behaviors usually result from random node failures or instable wireless medium, they cause high predicted behavior value and should be differentiated from real malicious behaviors.

Nash equilibrium [24] strategy is the most important solution in game theory. If the strategy s^*_{ing} of N_{ing} is the optimal response to the strategy s^*_{ed} of N_{ed}, and the converse is still established, then the strategy combination (s^*_{ing}, s^*_{ed}) is the equilibrium solution of this game. Any player cannot improve its own payoff by individually deviating from the selected equilibrium strategy, that is:

$$\begin{cases} u_{ing}\left(s^*_{ing}, s^*_{ed}\right) \geq u_{ing}\left(s_{ing}, s^*_{ed}\right) & \forall s_{ing} \in S_{ing} \\ u_{ed}\left(s^*_{ing}, s^*_{ed}\right) \geq u_{ed}\left(s^*_{ing}, s_{ed}\right) & \forall s_{ed} \in S_{ed} \end{cases} \tag{4}$$

Where u_{ing} and u_{ed} are the payoff functions of N_{ing} and N_{ed} respectively.

According to Table 1, the payoff function u_{ing} can be expressed as follows:

$$u_{ing} = p\left(-hE_m + E_c\right) + (1-p)\left(-hE_m + A_sCh/H\right) \tag{5}$$

Where p is the probability of cooperative behavior of node N_{ed}. Since the payoff function u_{ing} of N_{ing} is linear about the strategy h, according to the indifference in responses to the best strategy of N_{ed}, we can get:

$$-E_m + A_sC/H - pA_sC/H = 0 \tag{6}$$

Then we can get the equilibrium strategy of N_{ing} as follows:

$$p^* = 1 - HE_m/(A_sC) \tag{7}$$

Where $0.5 \leq A_s \leq 1$, which indicates that the monitored node N_{ed} always expects to be trusted by the monitoring node N_{ing}; $0 \leq HE_m \leq A_sC$, which indicates that the energy E_m consumed by N_{ing} for behavior monitoring should be no more than the minimal award $0.5C/H$ $(h = 1)$ when the malicious action of N_{ed} is captured.

From (7), we can see that if the expected trust A_s or the award C to N_{ing} for capturing the malicious behavior is higher, then N_{ed} tends to cooperate with N_{ing} by a larger probability for improving its own trust level while reducing the chance of rewarding to N_{ing}. If more energy needs to be consumed for behavior monitoring, then N_{ed} tends to cooperate with a smaller probability that reflects its selfishness when playing the game.

According to the indifference of N_{ed} in responses to the optimal strategy of N_{ing}, we can get:

$$-E_c + hE_m = -Ph/(V_sH) + hE_m \tag{8}$$

Then we can get the equilibrium strategy of N_{ed} as follows:

$$h^* = E_cV_sH/P \tag{9}$$

Where $h^* > 0$, which indicates that the relationship of size between the energy E_c consumed for cooperative action and the penalty $P/(V_sH)$ to malicious behavior depends on the predicted malicious behavior value V_s.

From (9), we can see that higher predicted malicious behavior value or more energy consumption for cooperative action will cause a longer monitoring duration. This indicates the expectation for malicious behaviors from N_{ed} is enhanced by N_{ing}. If a malicious behavior will cause a heavier penalty on N_{ed}, then a shorter duration of behavior monitoring will be conducted by N_{ing} as the selfishness during the game.

In conclusion, the equilibrium strategy of the dynamic behavior monitoring game exists, that is (h^*, p^*). Then the monitoring node N_{ing} will conduct monitoring task for duration h^* after it transmitted the data packet, and the value of h^* can be determined based on the predicted malicious behavior value to the monitored node N_{ed}. Moreover, N_{ed} will cooperate with N_{ing} based on the probability p^* which depends on its own expected trust value.

B. PARAMETERS COMPUTING

In our dynamic behavior monitoring game, the predicted value V_s of malicious behaviors to the monitored node is directly related to its current trust value T_s. Three cases may occur as follows:

- If $T_s = 0.5$, N_{ed} falls in a critical state of being trusted or untrusted. Then V_s will reach the maximum so that the following behavior of N_{ed} directly decides whether it can be trusted by N_{ing}.
- If $0 \leq T_s < 0.5$, with the decrease of T_s, V_s decreases until it reaches the left minimum v_{s-}. This case means

that when N_{ed} falls in the state of being untrusted, N_{ing} will reduce the trust expectation for N_{ed} while reducing the monitoring duration. The left minimum v_{s-} indicates N_{ed} is expected to revert to cooperative status at one point so that N_{ing} expends some energy cost to implement a brief behavior monitoring.

- If $0.5 < T_s \leq 1$, with the increase of T_s, V_s decreases until it reaches the right minimum v_{s+}. This case means that when N_{ed} falls in the state of being trusted, N_{ing} will reduce the expectation of malicious behavior to N_{ed} while reducing the monitoring duration. The right minimum v_{s+} represents a brief monitoring against the malicious behaviors result from the randomness of wireless medium and node failure or misbehavior.

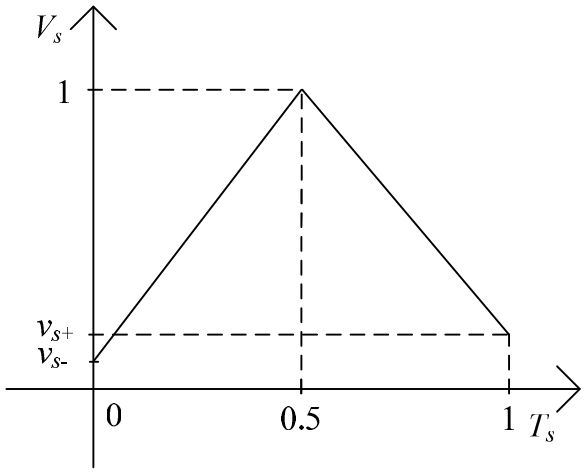


FIGURE 1. The relationship between predicted malicious behavior value V_s and trust value T_s.

For simplicity, we can use piecewise linear functions to description the relationship between V_s and T_s, as shown in Fig. 1. And the mathematical equation is shown as follows:

$$V_s(T_s) = \begin{cases} \alpha_- T_s + \beta_- & 0 \leq T_s \leq 0.5 \\ \alpha_+ T_s + \beta_+ & 0.5 \leq T_s \leq 1 \end{cases} \tag{10}$$

The expected trust value A_s of the monitored node N_{ed} can be calculated as follows:

$$A_s(T_s) = \begin{cases} kT_s & 0 \leq T_s \leq 0.5 \\ \log_a(T_s + 1) & 0.5 \leq T_s \leq 1 \end{cases} \tag{11}$$

Where k is increase rate of A_s when T_s is less than 0.5, and a is the base of logarithmic function that is bigger than 1.

Equation (11) indicates the monitored node N_{ed} has more expectation to enhance its trust value when it falls into the state of being untrusted, so that A_s increases linearly with the increase of T_s. When N_{ed} falls into the state of being trusted, it has less expectation to improve its trust value, then A_s increases logarithmically with the increase of T_s.

Considering the unreliability of wireless medium and the randomness of node failure or misbehavior, a probabilistic model is introduced to describe these characters. The Markov chain with two states can be used to model the time-varying channel [25]. Letting $L \in \{0, 1\}$ denote the channel quality, $L = 0$ means the channel falls in bad condition and $L = 1$ means the channel with good quality. The duration t_{cq} for sensor nodes in each state follows exponential distribution, and the probability density function is shown as follows:

$$p(t_{cq}) = \begin{cases} r_i \cdot e^{-r_i \cdot t_{cq}} & t_{cq} \geq 0 \\ 0 & t_{cq} < 0 \end{cases} \tag{12}$$

Where r_0 and r_1 denote the state frequencies corresponding to the channel in bad and good conditions respectively.

The average long-term fraction of time that the channel is in bad condition is given by $t_b = 1/(r_0 \cdot T_c)$, where $T_c = 1/r_0 + 1/r_1$. Then the probability p_{bc} for the channel in bad condition can be calculated as follows:

$$p_{bc} = t_b / T_c \tag{13}$$

Similarly, the duration t_{sf} of sensor failure follows exponential distribution, and the probability density function is shown as follows:

$$p(t_{sf}) = \begin{cases} h_i \cdot e^{-h_i \cdot t_{sf}} & t_{sf} \geq 0 \\ 0 & t_{sf} < 0 \end{cases} \tag{14}$$

Where h_0 and h_1 denote the frequencies of sensor failure happens and not. Then we can get the probability p_{sf} of sensor failures as follows:

$$p_{sf} = \left(\frac{1}{h_0 \cdot T_h}\right) \Big/ T_h \tag{15}$$

Where $T_h = 1/h_0 + 1/h_1$.

Considering both wireless channel quality and node failure or misbehavior, we can calculate the right minimum predicted value v_{s+} of malicious behaviors, which is shown as follows:

$$v_{s+} = p_{bc} + p_{sf} - p_{bc} \cdot p_{sf} \tag{16}$$

V. DETAIL OF OUR SECURE CLUSTERING PROTOCOL

Various attacks may occur during data routing process, and selective forwarding attack is the representative attack in WSNs which leads to serious damage to the monitoring system as data losing. In this section, we will design a trust based secure clustering protocol against selective forwarding attach. A trust evaluation mechanism will be presented firstly based on our dynamic behavior monitoring scheme, and then we give the detail of the secure clustering protocol.

A. TRUST EVALUATION

To evaluate the trust level of sensor nodes, beta probability density function will be used to descript the uncertainty [26] of trust evidences. Two parameters α and β of this function represent the binary trust outcomes, i.e. cooperative behavior and malicious behavior. The probability expectation value of beta distribution is defined as:

$$E(p) = \frac{\alpha}{\alpha + \beta} \tag{17}$$

Letting a and b represent the number of monitored cooperative behaviors and malicious behaviors based on our dynamic behavior monitoring scheme, then the expected probability E_c of cooperative behavior can be expressed as follows:

$$E_c = \frac{a+1}{a+b+2} \tag{18}$$

The expected probability of cooperative behavior for a node can be used to describe the reliability of this node, that is, the trust value V_t for a node can be calculated according to (18). For CH selection in clustered WSNs, a sensor node individually calculates the current trust value of each neighbor node based on the results of behavior monitoring. Moreover, to estimate the expected trust value A_s according to (11), a node has to calculate its own current trust value based on the numbers of packets that it has forwarded and not forwarded for all other nodes.

B. OUR SECURE CLUSTERING PROTOCOL

LEACH is one of the most famous clustering protocols in WSNs. Considering the malicious working environment, our dynamic behavior monitoring game based trust evaluation scheme will be introduced into LEACH to select trusted CHs. Then a new secure clustering protocol will be presented in this section. We call it as LEACH-T which contains many repeated rounds, and each one consists of topology formation phase and steady-state phase, as show in Fig.2.

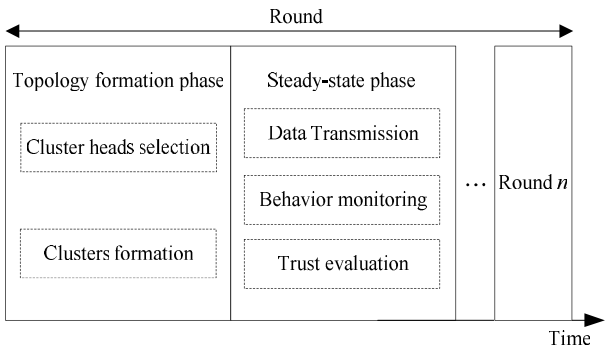


FIGURE 2. The procedure of our secure clustering protocol.

In the topology formation phase, both energy balance and network security will be considered. CHs will be selected firstly, then each normal node will select a suitable CH to join cluster. Assuming p_c is the probability of being the CH for each node, then any node i decides whether to be the CH according to a threshold $Th(i)$:

$$Th(i) = \begin{cases} \dfrac{p_c}{1 - p_c \cdot (r \bmod (1/p_c))} & \text{if } i \in G \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

Where r is the current topology formation round and G is the set consisting of the sensor nodes which have the eligibility to be CHs. If a node has not been a CH during the latest $1/p_c$ rounds, then it has the eligibility to be CH.

Any sensor node randomly selects a number within the range of [0, 1], it will be the CH if this number is less than the corresponding threshold Th. A node successfully selected as the CH will broadcast an election message. Then the normal node will select the nearest CH whose trust value is bigger than a threshold Th_t to be its own CH.

In the steady-state phase, sensor nodes begin to collect data from the surrounding environment. Then the normal node will transmit its data to the corresponding CH. Each CH will merge all member nodes' data with its own and forward the aggregated data to the BS. To avoid communication conflict on the wireless channel, each normal node will be allocated with an individual time slot by its own CH. Moreover, each CH transmits data to BS based on a randomly selected code division multiple access (CDMA) code.

After the data packet is transmitted, each normal node will monitor the behaviors of its own CH to update the trust value V_t and the trust threshold Th_t. If a cooperative behavior of a CH is monitored by its member node, the corresponding trust threshold will be increased by r_{in} times the absolute fore-and-aft difference of the updated trust value. If a malicious behavior is monitored, the trust threshold of the CH will be decreased by r_{de} times the absolute fore-and-aft difference to reduce the impacts of random wireless medium and node failure or misbehavior.

VI. PERFORMANCE EVALUATION

A. PARAMETERS SETTING

In this section, we will evaluate the performance of LEACH-T by comparing it with LEACH when no secure mechanism is integrated and when trust based secure mechanism with full-time behavior monitoring is adopted (LEACH-FT).

Some parameters used throughout the simulation process are listed in Table 2. Moreover, some other parameters used in our protocol can be calculated as follows: $\beta_- = v_{s-}, \alpha_- = (1 - \beta_-)/0.5, \alpha_+ = (v_{s+} - 1)/0.5, \beta_+ = v_{s+} - \alpha_+$.

B. RESULT ANALYSES

To conduct the simulation experiment via MATLAB platform, we treat the multiple h^* that calculated by (9) as the probability of successful behavior capture under the case that wireless channel quality is good and no node failure occurs. However, this probability will be decreased by half when wireless channel quality is bad or node failure occurs. If the two cases occur simultaneously, it will be decreased to a quarter. Moreover, we assume that each malicious node normally decides whether to be the CH according to (19). This is because we think that a malicious node is rational enough to avoid the obvious abnormal behaviors.

Network lifetime is one of the most important criteria for performance evaluation in secure clustering protocol. Fig. 3 gives the comparison of network lifetime among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes. We can see that the network lifetime in LEACH-T is shorter than that in LEACH, but longer than

TABLE 2. Parameter setting.

PARAMETER	Value
Probability to be CH p_c	0.05
Packet size (bits)	3000
Control packet size (bits)	300
Initial energy E_0 (J)	0.5
E_{elec} (nJ/bit)	50
E_{Tx} (nJ/bit)	50
E_{Rx} (nJ/bit)	50
ε_{amp} (pJ/bit/m^4)	0.0013
ε_{fs} (pJ/bit/m^2)	10
E_{DA} (nJ/bit/message)	5
E_m (nJ/round-trip time)	100
E_c (nJ/round)	1200
Trust threshold Th_t	0.5
P	0.0000012
C	0.0000016
H	3
a	2
r_0	0.2
r_1	0.8
h_0	0.1
h_1	0.9
$v_{s\text{-}}$	0.15
r_{in}	0.6
r_{de}	0.2

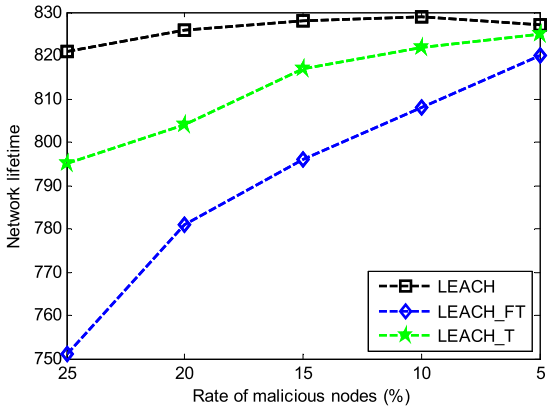


FIGURE 3. The comparison of network lifetime among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes.

that in LEACH-FT. This is because behavior monitoring is part-time conducted by sensor nodes in LEACH-T for trust evaluation. However, it is not happened in LEACH but carried out full time by sensor nodes in LEACH-FT. This figure also shows that the network lifetime in LEACH-T and LEACH-FT increase with the decrease of the rate of malicious nodes. This is because more sensor nodes have the chance to select a close CH to join cluster when less malicious nodes exist, then the average data transmission distance within the cluster can be decreased.

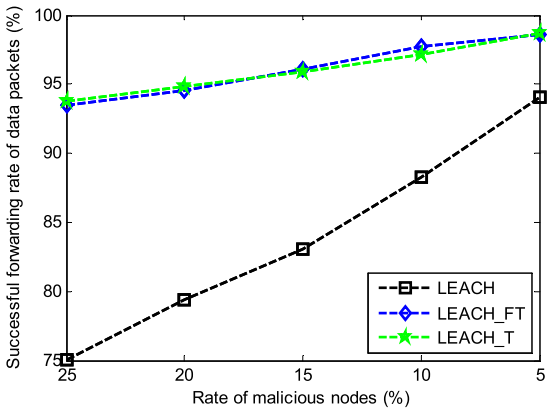


FIGURE 4. The comparison of data forwarding rate among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes.

Fig. 4 gives the comparison of data forwarding rate among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes. It shows that LEACH-FT and LEACH-T almost have the same data forwarding rate for each case of the rate of malicious nodes. This means our proposed dynamic behavior monitoring mechanism can achieve the same effect on behavior evidence collection with full time behavior monitoring scheme. From this figure, we can also find that LEACH-T and LEACH-FT have higher data forwarding rate than LEACH for each case of the rate of malicious node. This owes to the trust based secure mechanism that used in LEACH-T and LEACH-FT.

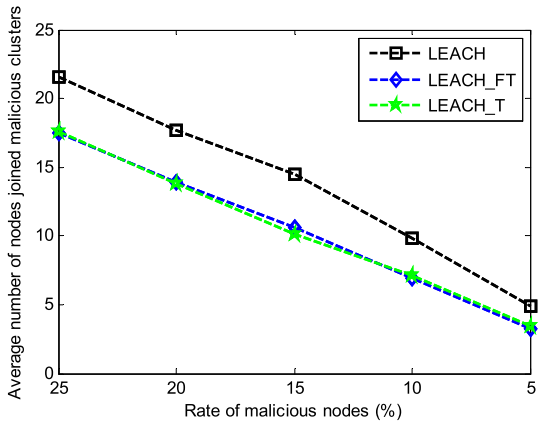


FIGURE 5. The comparison of average number of nodes joined malicious clusters among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes.

Fig. 5 gives the comparison of average number of nodes joined malicious clusters among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes. From this figure, we can see that for each case of the rate of malicious nodes, the average number of nodes that joined malicious

clusters in LEACH-T is equivalent with that in LEACH-FT, but smaller than that in LEACH. This is because sensor nodes in LEACH-T and LEACH-FT will evaluate the trust value of other nodes to select an appropriate CH before join clusters. Unfortunately, some sensor nodes still get the wrong option to join the malicious clusters in LEACH-T and LEACH-FT. On the one side, this is because malicious nodes are rational enough to improve their trust level if necessary. On the other side, normal sensor nodes hold gambler psychologies that selfishly hope to utilize the energy resource of malicious nodes.

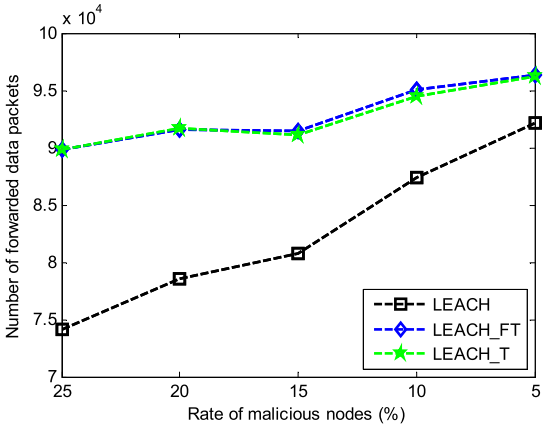


FIGURE 6. The comparison of number of successfully forwarded data packets among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes.

Fig. 6 gives the comparison of number of successfully forwarded data packets among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes. This figure shows that the number of successfully forwarded data packets in LEACH-T is equivalent with that in LEACH-FT but higher than that in LEACH. Correspondingly, the comparison of number of dropped data packets among LEACH, LEACH-FT and LEACH-T is given in Fig. 7. This figure shows that LEACH-T and LEACH-FT almost have the same number of dropped data packets, which is smaller than that in LEACH.

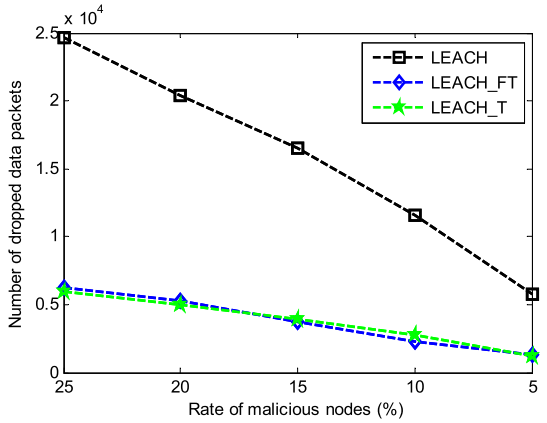


FIGURE 7. The comparison of number of dropped data packets among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes.

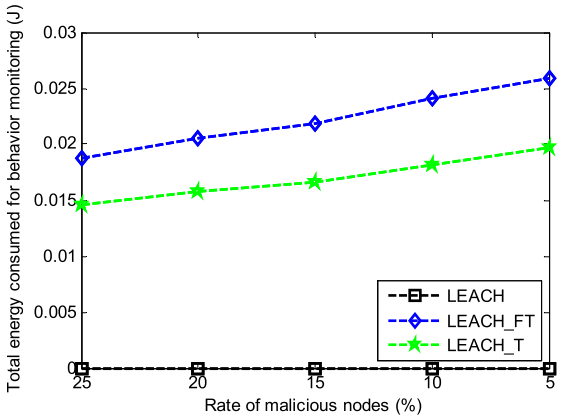


FIGURE 8. The comparison of total energy consumed for behavior monitoring among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes.

Fig. 8 gives the comparison of total energy consumed for behavior monitoring among LEACH, LEACH-FT and LEACH-T for different rates of malicious nodes. As behavior monitoring scheme is not used in LEACH, no energy will be consumed for it. However, for behavior monitoring in LEACH-FT, more energy has to be consumed than that in LEACH-T. From this figure, we can further find that the amount of energy consumed for behavior monitoring in LEACH-T and LEACH-FT increases with the decrease of the rate of malicious nodes. The is because more normal nodes exist when the number of malicious nodes decreases, then more nodes have to join the ranks of behavior monitoring that increases the total energy consumption.

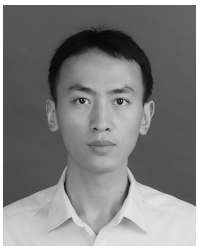
VII. CONCLUSION AND FUTURE WORK

In trust-based secure clustering protocols for WSNs, sensor nodes need to collect behavior evidences from CHs for trust assessment. To achieve a tradeoff between network security and energy consumption during behavior monitoring, we present a dynamic behavior monitoring game where sensor nodes determine the monitoring duration according to the predicted malicious behavior values to CHs. Moreover, the randomness of wireless channel quality and node failure or misbehavior is considered in the game so that the fuzziness of behavior evidences can be decreased effectively. Based on our dynamic behavior monitoring scheme, a trust assessment mechanism is proposed which is further introduced into clustering protocol for WSNs. And the simulation results show that the secure clustering protocol based on our dynamic behavior monitoring scheme can achieve a longer network lifetime than the one based on full time behavior monitoring mechanism, while the successful data forwarding rate is not reduced.

In our future work, we will devote to evaluate the trust level of sensor nodes in clustered WSNs. Some professional techniques will be used to reduce the fuzziness of behavior evidences, such as fuzzy logic, cloud model and pattern recognition.

REFERENCES

[1] Y.-W. Kuo, C.-L. Li, J.-H. Jhang, and S. Lin, "Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications," *IEEE Sensors J.*, vol. 18, no. 12, pp. 5187–5197, Jun. 2018.
[2] N. Mittal, U. Singh, and B. S. Sohi, "A stable energy efficient clustering protocol for wireless sensor networks," *Wireless Netw.*, vol. 23, no. 6, pp. 1809–1821, Aug. 2017.
[3] L. Yang, Y.-Z. Lu, Y.-C. Zhong, and S. X. Yang, "An unequal cluster-based routing scheme for multi-level heterogeneous wireless sensor networks," *Telecommun. Syst.*, vol. 68, no. 12, pp. 11–26, May 2018.
[4] R. Xie and X. Jia, "Transmission-efficient clustering method for wireless sensor networks using compressive sensing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 806–815, Mar. 2014.
[5] G. M. Borkar and A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks," *Wireless Netw.*, vol. 23, no. 8, pp. 2455–2472, Nov. 2017.
[6] A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Netw. Appl.*, vol. 21, no. 2, pp. 272–285, 2016.
[7] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2017.
[8] A. Ahmed, K. A. Bakar, M. I. Channa, A. W. Khan, and K. Haseeb, "Energy-aware and secure routing with trust for disaster response wireless sensor network," *Peer-Peer Netw. Appl.*, vol. 10, no. 1, pp. 216–237, Jan. 2017.
[9] J. Tang, A. Liu, J. Zhang, N. N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*, vol. 18, no. 3, p. 751, Mar. 2018.
[10] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7579–7592, Sep. 2016.
[11] H. Oh and C. T. Ngo, "A slotted sense multiple access protocol for timely and reliable data transmission in dynamic wireless sensor networks," *IEEE Sensors J.*, vol. 18, no. 5, pp. 2184–2194, Mar. 2018.
[12] H. Liao and S. Ding, "Mixed and continuous strategy monitor-forward game based selective forwarding solution in WSN," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, p. 359780, Nov. 2015.
[13] L. Yang, Y.-Z. Lu, Y.-C. Zhong, X.-G. Wu, and S.-J. Xing, "A hybrid, game theory based, and distributed clustering protocol for wireless sensor networks," *Wireless Netw.*, vol. 22, no. 3, pp. 1007–1021, Apr. 2016.
[14] J.-S. Fu and Y. Liu, "Double cluster heads model for secure and accurate data fusion in wireless sensor networks," *Sensors*, vol. 15, no. 1, pp. 2021–2040, Jan. 2015.
[15] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 58–69, Feb. 2014.
[16] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Netw.*, vol. 24, no. 3, pp. 777–797, Apr. 2018.
[17] H. Zhou, Y. Wu, L. Feng, and D. Liu, "A security mechanism for cluster-based WSN against selective forwarding," *Sensors*, vol. 16, no. 9, p. 1537, Sep. 2016.
[18] D. Agrawal and S. Pandey, "FUCA: Fuzzy-based unequal clustering algorithm to prolong the lifetime of wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 2, p. e3448, Jan. 2017.
[19] H. Marzi and A. Marzi, "A security model for wireless sensor networks," in *Proc. IEEE CIVEMSA*, May 2014, pp. 64–69.
[20] K. Guravaiah and R. L. Velusamy, "Energy efficient clustering algorithm using RFD based multi-hop communication in wireless sensor networks," *Wireless Pers. Commun.*, vol. 95, no. 4, pp. 3557–3584, Aug. 2017.
[21] A. A. Qasem, A. E. Fawzy, M. Shokair, W. Saad, S. El-Halafawy, and A. Elkorany, "Energy efficient intra cluster transmission in grid clustering protocol for wireless sensor networks," *Wireless Pers. Commun.*, vol. 97, no. 5, pp. 915–932, Nov. 2017.
[22] Y. Zhang, M. Liu, and Q. Liu, "An energy-balanced clustering protocol based on an improved CFSFDP algorithm for wireless sensor networks," *Sensors*, vol. 18, no. 3, p. 881, Mar. 2018.
[23] L. Yang, Y. Lu, L. Xiong, Y. Tao, and Y. Zhong, "A game theoretic approach for balancing energy consumption in clustered wireless sensor networks," *Sensors*, vol. 17, no. 11, p. 2654, Nov. 2017.
[24] T. Alskaif, M. G. Zapata, and B. Bellalta, "Game theory for energy efficiency in wireless sensor networks: Latest trends," *J. Netw. Comput. Appl.*, vol. 54, pp. 33–61, Aug. 2015.
[25] W. H. R. Chan *et al.*, "Adaptive duty cycling in sensor networks with energy harvesting using continuous-time Markov chain and fluid models," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2687–2700, Dec. 2015.
[26] R. Juliana and P. U. Maheswari, "An energy efficient cluster head selection technique using network trust and swarm intelligence," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 351–364, Jul. 2016.



LIU YANG received the B.S. degree in electronic information science and technology from the Qingdao University of Technology, Qingdao, Shandong, China, in 2010, and the Ph.D. degree in communication and information systems from the College of Communication Engineering, Chongqing University, Chongqing, China, in 2016. He is currently a Lecturer with the Chongqing University of Posts and Telecommunications. His research interests include wireless sensor networks and image processing.

YINZHI LU received the M.S. degree in communication and information systems from Chongqing University, Chongqing, China, in 2014. She is currently a Teaching Assistant with the School of Electronic Information Engineering, Yangtze Normal University. Her current research interests include wireless sensor networks and RFID technology.

SHENG LIU received the Ph.D. degree with the Communication and Aerocraft Tracking Telemetering Command Center, Chongqing University, in 2016. He is currently a Lecturer with Tongren University. His research is focused on array signal processing and statistical signal processing.

TAN GUO received the M.S. degree in signal and information processing and the Ph.D. degree in communication and information systems from Chongqing University, Chongqing, China, in 2014 and 2017, respectively. He is currently a Lecturer with the Chongqing University of Posts and Telecommunications. His research interests include biometrics, pattern recognition, and machine learning.

ZHIFANG LIAN received the B.S. degree in computer science and technology from Shanxi Normal University, China, in 2013, and the Ph.D. degree in intelligent signal processing from the College of Communication Engineering, Chongqing University, Chongqing, China, in 2017. She is currently with the College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications. Her research interests include electronic nose technology, artificial olfactory systems, machine learning, and intelligent algorithm.