IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 21, 2019, accepted September 15, 2019, date of publication September 30, 2019, date of current version October 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2944648

Adaptive Trust-Based Routing Protocol for Large Scale WSNs

NOR AZIMAH KHALID[1], QUAN BAI[2], AND ADNAN AL-ANBUKY[3], (Member, IEEE)
[1]Faculty of Computer and Mathematical Sciences (FSKM), Universiti Teknologi MARA (UiTM), Shah Alam 42300, Malaysia
[2]University of Tasmania, Hobart TAS 7005, Australia
[3]School of Engineering, Auckland University of Technology, 1010 Auckland, New Zealand

Corresponding author: Nor Azimah Khalid (nkhalid@aut.ac.nz)

ABSTRACT Due to the dynamic and uncertain behaviors of nodes in Wireless Sensor Networks (WSNs), reliable data delivery becomes challenging task. With the absence of global information and centralised decision maker, the nodes in distributed WSNs need to rely on the surrounding nodes. This reliance requires the nodes to select the most reliable partner to work with in relaying the packets. Thus, the evaluation criteria and evaluation process has become a crucial agenda. Recent approaches adopt the concept of trust in selecting the next forwarder. However, most of them are restricted to certain criteria and the evaluation are conducted for single node. Inefficient consideration on the factors involved and inability to have wider view of the network could lead to inaccurate selection of forwarder, which eventually causes packet loss or re-transmission that consumes more resources. In this paper, we present an Adaptive Trust-based Routing Protocol (ATRP) that encompasses direct trust, indirect trust, and witness trust that considers multiple factors (resources and security) in its trustworthiness using pairwise comparison. The proposed mechanism allows further evaluations on more potential nodes, at several hops that helps to balance the energy consumption and prolong the network lifetime. Simulation results demonstrate longer lifetime, less delay, less packet loss and low energy consumption when compared to existing protocols.

INDEX TERMS Adaptive routing, trust-based, routing protocol, multi criteria, WSNs.

I. INTRODUCTION

In the process of forwarding data from any wireless sensor node towards the sink, selection of the next forwarder is an important task for ensuring reliable data delivery. Large scale WSN involves large number of nodes where the data packets may need to be delivered via several hops, especially if the distance between source node (the node that initiate communication) and the sink is farther apart. An efficient distributed decision making for forwarder selection is thus required for effective routing.

In determining the next forwarder, several mechanisms have been proposed in existing literature. Among the most common approach is the cluster-based [1], [2], and [3] where a cluster head is elected to aggregate the data from the nodes around it. Even though this approach has proved its advantages, there are certain issues that come with it, in terms of energy consumption during cluster head election, re-election and broadcast of updates.

Adaptive forwarder selection has been proposed by considering multiple factors such as those suggested by [4]–[8], and [9]. Other existing mechanisms used in the next forwarder selection is through negotiation [10], game theory [11], [12], and learning-based [13]. However, these mechanisms are more applicable to network with resourceful nodes. It has proven that considering multiple factors in node selection decision is more effective than single factor consideration [14]. Here, most works involves multiple criteria for WSNs focuses only on resource related factors such the nodes residual energy and number of hop, which is not appropriate for applications such as in military an inaccessible area, as they are exposed to unpredictable behaviors due to security attacks, fault reporting etc. In such situations, later routing protocols had considered security factor in its forwarder selection. Nonetheless, these factors (resource and security), should not be considered separately.

There are existing trust models that consider both such as in [15], [16], ([17], [18], and [19]) but the number of such research is still very limited.

In this paper, a novel Adaptive Trust-based Routing Protocol (ATRP) is proposed. The protocol employs multiple

The associate editor coordinating the review of this manuscript and approving it for publication was Yue Zhang.

evaluations at multiple layers rather than single hop evaluations. The multiple factors consideration in ATRP balances the load distribution in the network and provides more accurate selection of the next forwarder. Please be noted that this paper is based on work also presented in [20].

II. RELATED WORK

Trust and Energy Aware Routing Protocol (TERP) for WSNs extends the routing mechanism of the ad-hoc on-demand distance vector (AODV) protocol that incorporates the trust, residual energy and hop count of the neighbour nodes [18]. The packet-forwarding behaviour of each of its 1-hop neighbours is monitored through promiscuous learning. The total trust is the weighted sum of three components: direct trust, indirect trust and probability of the expected positive behaviours. Direct trust is gained through the node's own experience with it's neighbours. It measures the number of correctly forwarded packets from each neighbour to the total number of packets received (i.e., the packet-forwarding ratio of each neighbour). Indirect trust constitutes the recommendations provided by other nodes. The expected probability of the positive behaviours refers to the expected future of the node based on its forwarding behaviour (the packet forwarding ratio) and is computed using the Beta probability density function. The nodes with low energy, and those suspected as malicious, are eliminated during the route recovery. A new route must be discovered whenever an intermediate node finds some energy deficiency and packet-forwarding misbehaviour by malicious nodes along the route. However, TERP has some restrictions in some applications due to its incapability to add or remove sensor nodes once the network is established.

The Direct Trust Dependent Link State Routing Protocol (DTLSRP) using route trusts for WSNs protects against routing attacks in WSNs by eliminating the non-trusted nodes and finding the best trustworthy route among the remaining nodes [19]. The parameters of the direct trust are calculated using the geometric mean. DTLSRP considers the basic features of link-state routing protocols and calculates the multiple hops along a route, but the trustworthiness calculation includes only the direct trust.

An integrated trust and reputation model (FIRE) proposed by [21] incorporates similar elements to a reputation model for gregarious societies (ReGreT) presented by [22]. The model integrates four types of trust and reputation: interaction trust (based on the past experiences of direct interactions), role-based trust, witness reputation and certified reputation. The agents likely performance is comprehensively measured based on these trust values in selecting appropriate interaction partners. The certified reputation (CR), rated the agent that rates its partners in past interactions. CR is a trust model that allows agents to provide third-party references about their previous performances to gain the trust of their potential interaction partners. CR is useful when direct information of the potential partners is not available, or when a selfish witness is unwilling to share the experience of a particular partner. The relevance of each certified rating is calculated by a rating-weight function. The relevancy of a given rating is measured based on the recency of the ratings (using exponential decay). All trust and reputation values in FIRE are combined into a single composite trust value, using the weighted mean method. Even though these two models incorporates a comprehensive trust evaluations, they are not considering the resource constrained network.

Rather than focusing on securing from specific attacks, there are some routing models which are more thorough aimed to enhance the security of data transmission and trust management for WSNs. In trust-based source routing (TSR), [23] used packet accuracy rate as evaluation criterion when computing the trust value of neighbour nodes. However, besides considering only packet accuracy rate in its computation, TSR also ignores recommendations from third-party nodes. Optimal route is completely executed by the sink node, which may effect the sink's residual energy and shorten the network lifetime.

In Efficient Distributed Trust Management (EDTM), [16], multiple factors were considered, including communication, data, and energy. The indirect trust calculation method used in EDTM provides accuracy of trustworthy routing selection. Unfortunately, the robust trust model lacked of relevant research on approaches of accessing trustworthiness of routes.

In [24], a cluster structure is adopted in dividing sensor nodes into clusters based on distance and adjacent relationship during the network setup phase, which is an improvised version of trust-aware routing protocol with multiattributes (TRPM) [25]. TRPM considers direct trust: (communication trust metrics, i.e., packet receive feedback and packet forwarding, data trust metrics (perceived data accuracy and packet accuracy), energy trust metric (residual energy ratio and energy consumption rate variation), and recommendation trust (response of recommendation request and recommendation accuracy). The indirect trust value in TRPM is measured by comparing the recommendations from neighbours with the direct trust value of evaluated nodes. As it is a cluster based approach, TRPM involves several phases including cluster division, cluster head election, and cluster head identification broadcasting before selection on trusted nodes take place, which may be cost consuming for WSN.

Based on the literature review, it is concluded that existing distributed solutions still demand for efficient and reliable mechanisms for the next forwarder selection. The motivation of this chapter is then based on several factors below:

- In large scale networks, the factors choose in making decision for data forwarding is crucial. Researches have shown that considering multiple factors leads to better decision. However, not many existing routing protocols in WSNs consider various factors in their decisions. Besides, the limited number of multi criteria routing protocols lack some flexibilities and focus only on certain isolated factors. For example, existing routing protocols only focus either on energy efficiency or security.

Also the factors considered are focusing on specific network measures such as either coverage or energy efficiency. Due to the nature of open systems, the nodes in the network are expose to many uncertainties. Thus, the criteria considered should be constructed in such a way that it could handle such uncertainties, rather than handling a specific network measure.

- Most studies on trust management has been targeted for general ad hoc networks and peer-to-peer networks with powerful hardware platforms but not for resource constrained network, such as WSNs. Thus, most of trust based routing approaches only focusing on selecting most trusted neighbours irrespective of their energy resource, which undermines the energy conservation goal in protocol design.
- WSN normally covers a large area of network, where the route from source to the sink involves multiple hops, due to limited coverage of each node. In many existing researches, a node only needs to decide the next neighboring node it should forward the data packet (1-hop neighbours). To choose its next-hop node, source node only considers the trustworthiness of its single hop neighbors. In the absence of global information and the presence of such uncertainties, the node selection that considers more than 1 hop node becomes a crucial agenda in order to give a better or wider perspective of the network. For example, if the packets were sent to capable nodes with incapable neighbours, retransmissions may be required or the packets may be dropped.

The objective of adaptive trust-based routing protocol (ATRP) is to propose an efficient trust-based routing protocol for selection of relay nodes in distributed and decentralized wireless sensor network based on multiple trust factors and multi levels trust evaluations. In order to achieve this objective, ATRP embed several features as given below:

1) Multi criteria decision making: Several trust metrics are identified according to different network performance which may lead to better decision as more uncertainty aspects are considered in the decision.
2) Resource aware mechanism: ATRP provides resource aware mechanisms in several ways. First, by considering resource such as energy as its trust metrics could reduce the need for retransmission. Second, by enabling control mechanisms in terms of number of interactions in order to limit the flooding effect in the network. Third, the decision provides by lower layer evaluator reduced the higher layer evaluator's task, thus allow them to sustain longer in the network.
3) Multi-hop evaluations could assist in better decision making as the evaluator will have larger view of the network, i.e., having information about more nodes in the network.

III. THE PROPOSED ADAPTIVE TRUST-BASED ROUTING PROTOCOL (ATRP)

Adaptive Trust-based Routing Protocol (ATRP), is a hierarchical trust-based routing protocol for large scale and decentralized wireless sensor networks. It consists of several features highlighted in previous sections. They are multiple factors considerations, multi-hop evaluations and local decision making.

The network considered in ATRP is homogeneous, where all agents have the same capability and initial energy. When routing packet from source to destination which is far away, multi-hop is required, where packets are sent to intermediate nodes, and then forwarded to the destination. However, routing in such environment is challenging as nodes are exposed to coverage hole issues, which may due to nodes depletion in the network or obstacles existence along the route.

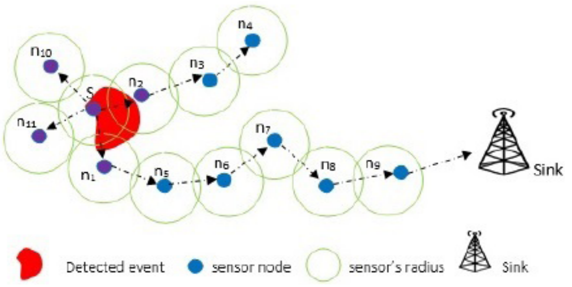

FIGURE 1. **Possible scenario of 1-hop evaluations.**

Figure 1 illustrates the scenario of 1-hop evaluations. Without having the information about nodes at further layers forward, S only relies to this direct observations. The selection may not be optimal one as S are not aware that n_2's neighbor, i.e. n_3 is connected to a neighbour (n_4) that is not connected to the sink. Thus, packet sent via n_2 will never reach the sink. S may not choose n_1 even though n_1 has neighbours that are connected to the sink. This is due to lack of information about nodes at other layers.

The sensor nodes can be modelled as autonomous agents which are responsible in delivering packets from sources to the destination (sink). Hence, the whole wireless sensor network can be considered as a Multi-agent System (MAS). Being an autonomous system, requires all nodes to be self-organized and react dynamically with their environments. However, the uncertainties exist due to several reasons, such as weak coverage, low connectivity, depleting resources etc. The nodes should be able to make their own decision in a distributed manner, towards these uncertainties based on limited information. Thus, by having more information about the candidate (through direct observation and through the third parties), will give better idea to the recruiter, that could leads to better selection decision, even though there are certain level of risks in that decision making (bias information etc.).

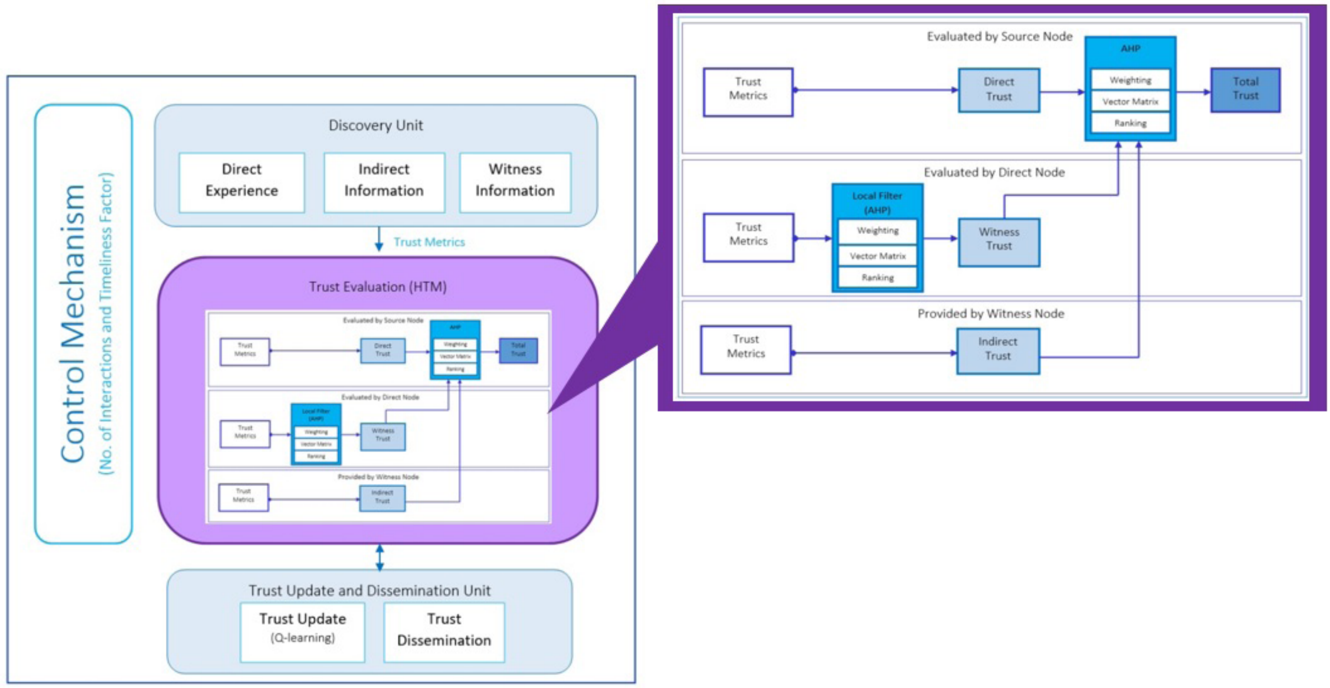

FIGURE 2. Components of ATRP and relationships between them.

A. DEFINITIONS

Before explaining further, it is necessary to understand several important and related terms in ATRP. The network in our model is considered as a complex system comprising a number of sensor nodes (or agents).

Definition 1: The network: A WSN is defines as connected undirected weighted graph $G = (V, E)$, where V is group in the network comprises of agents, i.e. $V = a_0, a_1, a_2, \ldots a_n$ and $E = e_1, e_2, \ldots . e_m$ is a set of edge in group. The edge, $e_k = (a_i, a_j)$ denotes the communication links between sensor a_i and sensor a_j (they are in each other's radio transmission range).

Definition 2: If the Euclidean distance between sensor node S and any sensor node n_i is not greater than r_s, then n_i is called direct node of sensor node S. If the Euclidean distance between direct node n_i and n_j is not greater than node n_i sensing radius r_s, then n_j is the witness node of direct node n_i.

Definition 3: Malicious node is defined based on packet forwarding ratio between node i (as sender) and node j (as receiver), i.e. $|\Sigma Fwd_{correctij}|/|\sum Rcv_{packetij}|$, where $\Sigma Fwd_{correctij}$ is total number of correctly forwarded packet by node j and $\sum Rcv_{packetij}$ is total number of receive packets by j from i. A node is identified as MN if the value of packet forwarding ratio is $< Th_{FwdRatio}$, where $Th_{FwdRatio}$ is threshold value of packet forwarding ratio.

Definition 4: Trust metrics: There are various metrics considered in ATRP. The metrics are classified as main metrics (also called main criteria (MC)) and sub-metrics (sub-criterion (SC)). The metrics are structured in hierarchical level (HL), where, in $HL_i \subset (MC_1, MC_2, \ldots MC_n)$ and each MC may consist SC, such that $MC_i \subset (SC_1, SC_2, \ldots SC_n)$. Each SC is associates or link with n Alternatives. Thus, a hierarchy can be redefined as $HL_i \in (MC_1 \subset (SC_1, SC_2, \ldots SC_n), MC_2 \subset (SC_1, SC_2, \ldots SC_n), ..MC_n \subset (SC_1, SC_2, \ldots SC_n))$.

B. STRUCTURE OF ADAPTIVE TRUST-BASED ROUTING PROTOCOL (ATRP)

ATRP deals with discovering neighbouring nodes during the transmissions, conduct trust evaluation based on monitored and gathered values and dissemination of trust value and trust recommendation. Thus, ATRP is made up of three components shown in Figure 2. These are: discovery, evaluation and dissemination units. In addition, control mechanism unit in ATRP is responsible to support the implementation of ATRP in WSN environment.

1) DISCOVERY UNIT

In discovery unit, nodes learn about their neighbours' behaviours via direct observations and through recommendations by the third parties. Requested nodes (evaluators) will determine the information required from their neighbours that is necessary for the selection decision. Upon monitoring, related nodes may discover certain behaviours of its neighbours. Thus, this phase is also known as route discovery phase. Algorithm 1 shows the algorithm for forwarder selection in ATRP.

Algorithm 1 The Forwarder Selection Algorithm

```
Input: Selection Metrics
Output: Ranked and Select Forwarder
for For all episodes do
    Source send ReqD to nodes in Radius $\leq$ RadiusSource
    Nodes at Radius $\leq$ RadiusSource, i.e., Direct Node check its Capability
    if Capability > CapabilityThreshold then
        Send ReqW to nodes in Radius $\leq$ RadiusDirectNode
        Wait for reply from $N_{min}$ number of witness, i.e., RlyW
    end
    for Received RlyW from witness do
        Direct node compute witness trust (WT) for $N_{min}$ nodes
        Sent RlyD $< WT_i, Rep_{D-i}, Direct_{Metric} >$ to Source
    end
    for Receive RlyD from Direct node do
        Source compute Trustworthiness
        Rank Forwarder in Decreasing order
        Send DATA to selected Direct nodes and its witness
    end
end
```

2) TRUST EVALUATION UNIT

The second component of ATRP as illustrated in Figure 2 is the Trust Evaluation unit. The Trust Evaluation unit plays an important role in determining the nodes' level of trust. Here, trust and reputation evaluation and integration is performed. As previously mentioned, in ATRP, the output provides by the lower layer evaluators (i.e., the direct node and witness nodes) are used as input by the higher layer evaluator (the source node) who is then making the final selection decision.

There are three trust values that contribute to total trust in our forwarder selection. Direct Trust (DT) is a trust value calculated based on direct communication between the source (evaluator) and its direct (immediate) neighbours and also between direct nodes and its direct neighbours (witness nodes). Indirect Trust (IT) is a trust value of the evaluated node, calculated or gained from indirect neighbours of the evaluator. The indirect neighbours of the evaluator are direct neighbours of the evaluated node. Some information may not be available through direct communication. For example, the previous performance of the evaluator in any interaction in the past can be assessed through other nodes indirectly. This also applies in the case of the source node having no previous experience with the direct node. The indirect trust value is about communication behavior between nodes, i.e., whether evaluated nodes have successful or failure of communication (in transmitting any data etc.). The Indirect Trust value is forwarded by the direct node to the source node for computation of total trust. Witness Trust (WT) is trust of indirect neighbours (direct neighbours of the evaluated node) given by the evaluated node. Thus, to find the best forwarder, the source node will consider direct trust, indirect trust and witness trust in its total trust calculation.

TABLE 1. Main criteria and sub-criteria (the trust metrics) considered in ATRP.

Criteria	Sub-Criteria	Desirability
Reliability	% Packet Delivery Rate (PDR) [28]	HB
	Probability of Not Fail [29]	HB
Coverage	No. of Nodes	HB
	Coverage Detection Level(CDL) [30]	HB
Energy Efficiency	Residual Energy (E_{res})	HB
	Distance between DM-Witness	LB
	Distance between Witness-Sink	LB
	Throughput [31]	HB
Reputation	Success/Failure Rate	HB/LB
	Aging	HB

Note: HB- Higher is better, LB-Lower is better.

The trust metrics considered in ATRP is shown in Table 1. At each layer, the trust is computed using the Analytical Hierarchical Process (AHP) method to determine the score for each evaluated node.

After the total scores of all alternatives have been calculated, the decision maker (source node) should choose the alternatives that have high scores.

$$TotalTrust = DT + IT + WT \tag{1}$$

Table 1 shows the main criteria and sub-criteria that are used in calculating the alternatives. At the higher level, the four main criteria comprised of reliability, coverage, energy efficiency, and reputation. For each of the main criteria, there are several sub-criteria (metrics) considered, as illustrated in Table 1 second column. The desirability indicates whether higher (HB) or lower (LB) values are preferred for each criteria (and sub-criteria). For example, in terms of reliability, higher packet delivery rate and higher probability of not failing are preferred. The nodes that follows the desired criteria will have better chance to be selected. Instead of weighted sum that is mostly used in existing routing protocols for WSNs, ATRP uses the pairwise comparisons that provide more accurate weight to each preference [26]. The local weight is generated for the sub-criterion and is multiplied with global weight (gained by the main criterion). Alternative that has highest value will be selected as the next hop node.

Figure 3, demonstrates the hierarchies in ATRP, where each layer consists of several main criteria (MC) and sub-criterion (SC). n alternatives are to be evaluated based on these criterion using analytical hierarchy process (AHP).

3) TRUST UPDATE AND DISSEMINATION UNIT

The third component of ATRP is the Trust Update and Dissemination unit. Algorithm 2 shows the algorithm for updating and disseminate the information on successful or failure transmission. In distributed network, nodes do not have the ability to monitor current conditions or changes

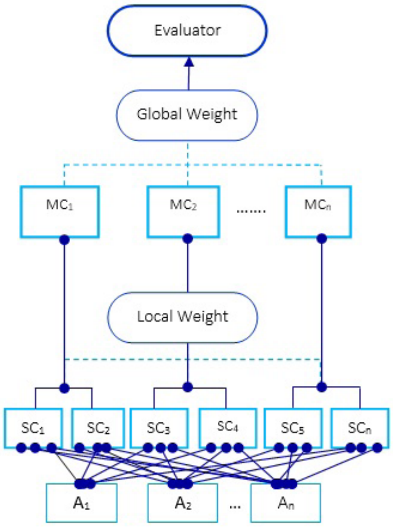

FIGURE 3. Illustrations on trust evaluations on *n* alternatives, involving various main criteria (*MC*$_1$ to *MC*$_n$) and sub-criterion (*SC*$_1$ to *SC*$_n$).

Algorithm 2 The Updating Forwarder Algorithm

```
Input: Aging, Q value, Confidence parameters
Output: Updated Forwarder Selection
for For all episodes do
    if Receive Req or requires routing service (source node) then
        if Aging (Equation 10) $\leq$ AgingThreshold then
            Send packet to nodes that have CL $\leq$ CLThreshold
        end
    end
    Update Qvalue using Equation 3
end
```

of the rest of the network. As nodes are not rechargeable, it will deplete through time. Nodes in this situation learn about its network based on state and actions it takes previously. Trust values are stored at each evaluating node's. Whenever evaluator receives packet to be transferred, it will either transfer the packet based on route in its trust table (if exist) of else it will create a new trust table. Trust update and dissemination unit is responsible if there is trust table exits. The dynamic behavior is monitored by each node. The trust values are not periodically updated but only when there are changes. Trust values that are expired will be removed. Up-to-date information will be sent by direct or indirect nodes whenever required by source nodes. The trust value in ATRP is updated using Q-learning technique, which is explain in below section, where the agent learns an action-utility function, labelled as Q(s,a) that tells the value of doing action a in state s. The Q-learning is implemented by Equations 3 to 3

$$Q*(s_t, a_t) = r_t + \gamma \sum_{s_{t+1} \in S} (P^{a_t}_{s_t s_{t+1}} max_a Q*(s_{t+1}, a)) \tag{2}$$

$$V*(s) = max_a Q*(s_{t+1}, a) \tag{3}$$

Thus, at each time step t, an action a is selected for the current state s, and the successor state (s') is observed. The typical value for γ is within [0.5, 0.99].

In the proposed approach, both successful and failure transmissions contributes to the calculation of the Q-values. The two functions, as in [13], comprises $Reward^i_j$ as in Equation 4 and $Penalty^i_j$ as in Equation 6. If the packet forwarding attempt from a_i to a_j is successful, the agent will be rewarded. The reward function is shown in Equation 4.

$$Reward^i_j = -g - \alpha(c(a_i) + c(a_j)) \tag{4}$$

In Equation 4, g is the constant cost when a_i tries to forward a packet. Because of the importance of the term $-$g, its weight is set to be 1, and the α weights lower than 1. Based on the guideline in, α value can be set to 0.5. $c(a_i)$ and $c(a_j)$ are cost functions of residual energy of a_i and a_j respectively, which can be calculated by using Equation 5.

$$c(a_i) = 1 - ERes_i/EInit_i, \tag{5}$$

where $ERes_i$ is the residual energy of a_i and $EIniti$ is a_i's initial energy.

On the other hand, if the forwarding attempt from a_i to a_j fails, agent will be penalized. The penalty, ($Penalty^i_j$) is defined as the equation below.

$$Penalty^i_j = -g - \beta c(a_i), \tag{6}$$

where β is weight for the cost function that can be tuned. The value of β can be set less than 1. According to, the value for β can be set to 0.5.

r_t is a accumulation of failure and success of node i towards node j. Based on Equations 4 and 6, the total reward given by i to j, denoted as r_t can be calculated by using Equation 7.

$$r_t = Reward^i_j + Penalty^i_j \tag{7}$$

IV. CONTROL MECHANISMS UNIT

Control mechanisms unit in ATRP is responsible to ensure that the trust value is valid and reliable. There are three components in control mechanism unit, i.e. number of interaction, decay time factor and timeliness measurement.

A. NUMBER OF INTERACTIONS

In randomly deployed network, it is impossible to determine how many interaction exist between nodes. Due to non-uniformity of the deployment, dense areas may have more nodes connected to the evaluator (the source node or the direct node) compared to sparse area. ATRP assumes that every trustee agent starts with no prior interaction experience with trustee agent and direct trust evidence will gradually accumulates over time [31]. Level of confidence, represented as γ, is used to indicate the weight of interactions, where, as the number of interactions with trustee increase, the value of γ also increases according to Equation 8:

$$\gamma = \begin{cases} \frac{N^B_C}{N_{min}}, & \text{if } N^B_C < N_{min} \\ 1, & \text{otherwise} \end{cases}, \tag{8}$$

where N_C^B is the total number of direct observations of a C's behaviour by a truster agent B, and N_{min} is the minimum number of direct observation required to achieve a predetermined acceptable error rate ε and confidence level ϑ. N_{min} (i.e. the minimum bound of interactions) can be calculated using Chernoff Bound Theorem, as in Equation 9:

$$N_{min} = -\frac{1}{2\varepsilon^2} ln \frac{1-\vartheta}{2}, \tag{9}$$

where ε refers to the deviation of the estimator from the actual parameter, and can be considered as a fixed parameter and ϑ is the confidence level. The length and number of interactions influence the trustworthiness of the nodes. Trust may not be established if the number of interactions is too short. On the other hand, in the dense area, if number of interactions is too high, more energy and resource will be consumed. In ATRP, the Chernoff Bound Theorem is used in monitoring the number of interactions between nodes, i.e., it is used as threshold value for number of interactions, to balance the consequences of number of interactions in the network.

B. DECAY TIME FACTOR

Another factor considered in ATRP control mechanism unit is the recency of the trust information. A nodes's historical trust values should be taken into account to measure its current trustworthiness. The dynamic behaviors of WSNs such as leaving or joining the network, due to battery depletion etc., require for the trust values of sensor nodes to be updated accordingly. However, the update frequency should be controlled as trust value should not be updated too often as it may waste a lot of energy. In addition, update cycle time that is too long would not reflect current behaviors of the object node efficiently.

As the trust value will decrease with the elapse of the time, mechanism to track the relevance of trust value is necessary. ATRP uses an exponential decay time factor is use to update the trust value. This mechanisms is also used in several studies including in [16] and in [32]. The exponential decay time factor (Equation 10) is use in ATRP. When the value of $\gamma \ll$ less 1, it means that the results of recent interactions are much more important than those of older ones.

$$\gamma = e{-}^{\rho \times (t_c - t_{c-1})}, \tag{10}$$

where t_c stands for the current time and t_{c1} represents the time when the last interaction happens.

C. MEASURING TIMELINESS

In applications involving resource constrained nodes, timeliness is an important factor to be considered. ATRP embedded timeliness factors in it's control mechanism unit to ensure that receive packet is still meaningful. An interaction may be considered fail if no result is received after a predetermined deadline. The timeliness discount factor in ATRP is measured using Equation 11 :

$$f_{td}(T_{end}) = 1 - \frac{T_{end} - T_{start}}{T_{dl} - T_{start}} \tag{11}$$

The closer T_{end} is to the time the interaction started (T_{start}), the closer $f_{td}(T_{end})$ should be to 1. On the other hand, the closer the T_{end} is to T_{dl}, the closer $f_{td}(T_{end})$ should be to 0.

V. SIMULATION RESULTS

This section analyses the performance of the ATRP in a simulation conducted on the MATLAB software platform. The details of parameters used in ATRP simulations are listed in Table 2. The simulation is conducted for 10 rounds where each round is equivalent to 100s. The aims of the simulation were 1) to observe the ATRP performance under different number of nodes, workloads and in the presence of malicious nodes, and 2) to compare the ATRP performance with those of other existing homogenous multi criteria and single-hop node evaluation routing protocols (TERP and DTLSR).

TABLE 2. Simulation parameters.

Simulation time	1000s
Deployment area	$1200x800m^2$
Number of sensor nodes	100
Number of malicious nodes	1-20
Communication range	30m
Length of packet	No. of Nodes
β, γ, α	0.5, 0.5, 0.5
Initial energy	50Joules
Coverage hole threshold	0.9

This subsection presents simulation results of ATRP against TERP and DTLSR. The performance in terms of energy, throughput, packet delivery ratio and average end to end delay is evaluated by varying the number of nodes in the network, considering various network load, and considering the existence of malicious nodes in the network.

1) CONSIDERING DIFFERENT NUMBER OF NODES

ATRP provide better and more accurate information by knowing few hops away nodes conditions. Packet drop due to unreliable and unavailable nodes to reach the sink can be avoided. The multi criterion used in ATRP provides better assistant in node selection. Node has the ability to determine whether it is capable to perform packet delivery or not. In addition, reputation given by other nodes may confirm the reliability of others.

ATRP is an adaptive protocol, that performs well even when large number of nodes were deployed, as shown in Figure 4. This is because they are selected based on its current conditions. When a frequently used nodes no longer performing better, source node will select other nodes that have higher capability. In Figure 4a, more energy is consumes when more nodes were deployed in the network. Figure 4b shows the throughput a higher throughput in ATRP compared to TERP and DTLSR. The throughput in ATRP is not much effected with the increase number of nodes. However, the throughput in TERP and DTLSR decreased with the increase number of nodes in the network. More packets are successfully delivered in ATRP Figure 4c compared to the other two protocols. However, the packet delivery ratio in ATRP is not much influenced by the increasing number of nodes. Instead, the packet

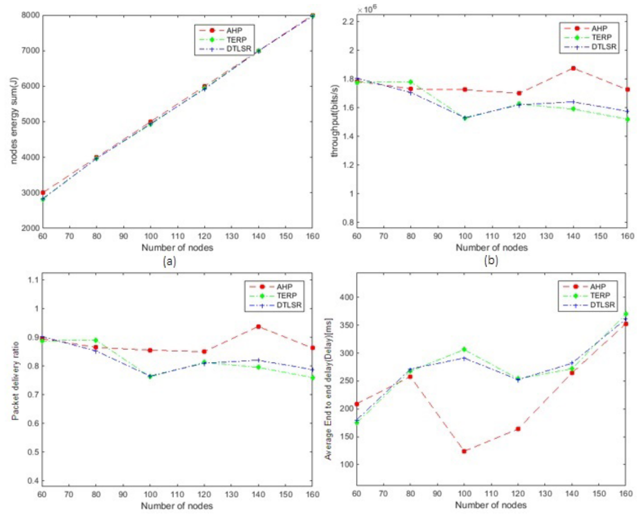

FIGURE 4. Performance comparison considering different number of nodes in ATRP, TERP and DTLSR.

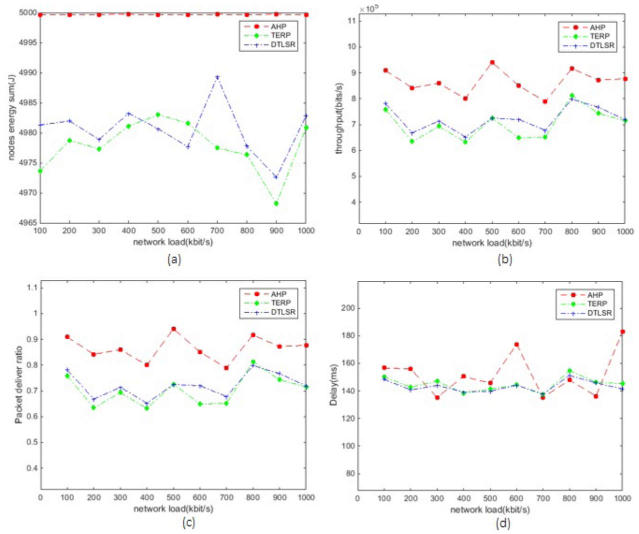

FIGURE 5. Performance comparison considering various network load (200 to 1000Kbps) in ATRP, TERP and DTLSR.

delivery ratio in ATRP increases with the increase number of nodes, which is contrast to the other two protocols. The average delay in ATRP is less compared TERP and DTLSR and gradually increases when the number of nodes in the network increased. The delay in TERP and DTLSR are higher and increase with the number of nodes.

2) PERFORMANCE EVALUATION UNDER VARIOUS NETWORK LOADS

This subsection presents the performance evaluations of ATRP, TERP and DTLSR under different network loads. The performance is evaluated in terms of energy efficiency, throughput, packet delivery ratio and average end-to-end delay.

Figure 5 shows the performances of ATRP, TERP and DTLSR in terms of energy, throughput, packet delivery ratio and delay under various network load. Based on Figure 5a, it is observes that in terms of energy consumption, DTLSR consumes the most, followed by TERP. The least energy is consumed in ATRP. In addition, the energy is uniformly consumed under the various network load (100 to 1000Kbps). A high throughput is observes in ATRP. DTLSR outperforms TERP with slight difference in terms of throughput (Figure 5b). Packet delivery ratio in ATRP is the highest among all. The performance of DTLSR in terms of packet delivery ratio is also higher than TERP when various network load is considered (Figure 5c). However, the performance of ATRP in terms of average end to end delay is higher than TERP and DTLSR as shown in Figure 5d.

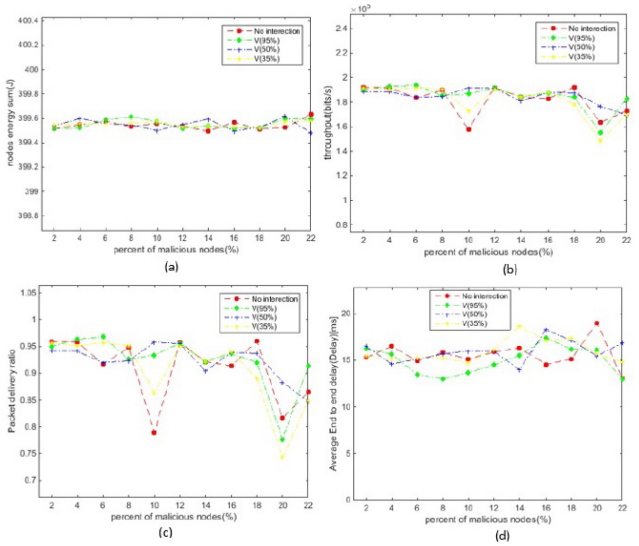

FIGURE 6. Performance comparison considering various number of malicious nodes in the network.

Based on results in Figure 5, ATRP outperforms the TERP and DTLSR in terms of energy, throughput and packet delivery ratio, under various network load. ATRP selects the forwarder in an efficient way that allows the network load to be distributed in more balance manner. Due to the fair load distribution among nodes, the packets are able to be delivered smoothly and successfully. The energy consumption is less due to its control mechanisms that reduce the flooding effects in the network.

3) PERFORMANCE EVALUATION UNDER VARIOUS NUMBER OF MALICIOUS NODES

Figure 6 shows the performances in terms of energy, throughput, packet delivery ratio and delay when certain percentage of malicious nodes exist in the network. A node is considered as malicious node if it's packet forwarding ratio is less than the packet forwarding ratio threshold value (Definition 2). Due to this, randomness of results is expected, especially in scenarios when the number of interaction is not controlled (labeled as no interaction in the gure) and when the level of the expected interaction expected is minimal (35%).

This can be seen in Figures 6b and c. However, based on the results, it is observes that ATRP performs well even with the existence of malicious nodes. The selection criteria considered in ATRP enable it to detect and eliminate malicious nodes in the network.

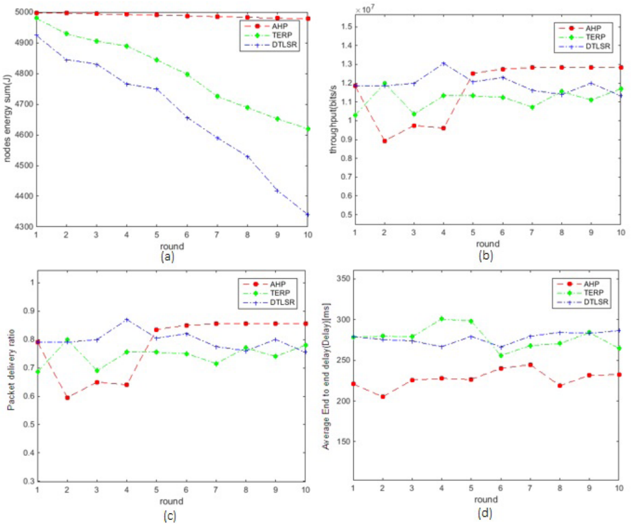

FIGURE 7. **Performance comparison in 10 rounds when 10 malicious nodes exist in ATRP, TERP and DTLSR.**

4) CONSIDERING EXISTENCE OF MALICIOUS NODES

Figure 7 presents the simulation results of ATRP against TERP and DTLSR, considering the existence of malicious nodes in the network. Figure 7a demonstrates the average of participating nodes remaining energy in the network. The higher the values for y-axis indicates more energy efficient the protocol is, i.e. less energy were consumed in routing packets from source to destination. Among the three schemes, ATRP performs better as the remaining energy is still high. Nodes remaining energy in TERP is higher than DTLSR. Energy is consumes when sending request and receives reply, due to re-transmission, computations and transmission of data.

ATRP outperforms the other two schemes due to its comprehensive considerations in its decision making process, besides considering factors considered in TERP and DTLSR, such as energy, distance (hop count) and trust. In these communications, ATRP provides several mechanisms such as control of number of interactions, local decision by direct and source nodes, multi criteria considerations and learning mechanism in its decision. These mechanisms helps in ensuring appropriate number of interactions required (more interactions may not be necessary and consume more energy), lower layer decision reduces burden of higher layer decision maker and reduce the number of potentials to be evaluated, criteria used in selection considers several aspects allows nodes to avoid malicious nodes at the earliest and learning based reduce the number of request and reply required as nodes learn to make decision based on its existing local information rather than asking for information every time request is sent to them. More energy is consumes in DTLSR could due to its reliance on only direct trust even tough several factors were considered in evaluation of the direct trust.

In TERP, there is no control mechanism such as in terms of number of interactions. Thus more energy is consumes in interactions between nodes. In addition, for every error or changes in the route, route maintenance phase will be involved which requires messages to be sent to all related nodes and route discovery need to be re-initiated, thus, more energy is consumes.

Figure 7b shows the throughput in all three schemes. DTLSR demonstrates better throughput than followed by TERP and ATRP. However, the throughput decreases after several rounds. Contrary, the throughput in ATRP increases after several rounds. The trust estimation and attack capability in TERP is more accurate, incorporated several aspects such as probability for positive behaviour of nodes, the direct and indirect trust. TERP combines energy awareness with the concepts of trust in its route setup to allow selection of efficient trusted nodes which significantly increase the throughput. The result exhibits reduced throughput performance of DTLSR as it only relies on direct trust and overlook the energy preservation aspect. Thus, it also leads to the increased number of dead nodes. As the routing of these two protocols only rely on the trust values of one-hop neighbours, the probability of selecting the best path is low as they are unaware about the rest of the network topology.

In a dense network, ATRP are expose to more potential forwarder and yet only credible and reliable providers (considering several aspects and criteria). In ATRP, as the nodes learn the performance of their neighbours, malicious nodes can be detected and avoided earlier. Thus, packets are relayed through other reliable nodes. The throughput in ATRP is higher also due to evaluation mechanism provided for multiple hops rather than a single hop, i.e. by making decisions about several hops away would be better rather than relaying through a single hop node which have no neighbours, would cause packet drop etc.

Figure 7d presents the evaluation results of all schemes in terms of average end-to-end delay. ATRP outperforms the other two schemes because the routing decision in ATRP requires nodes to select energy efficient, good coverage, reliable and good reputation nodes which allow the packets to be relayed smoothly through an optimal nodes, thus, minimizes the average end-to-end delay. In DTLSR, node is selected if it provides the highest reliability and also the shortest path. Also, the nodes with shortest path will be selected when the trust levels of all the nodes are equal. If there is no node within shortest distance between source and destination, longer paths may be selected. Thus, the end-to-end delay is increased as longer paths are more disposed to failure and require more route request and recoveries. These process cause network congestion that restrict the availability of bandwidth for data packets. In TERP, node selection is based on composite routing metrics that include energy efficiency, shortest and trusted routes which may keep a consistent flow of packets longer, thus, minimizes the average end-to-end delay. The performance in terms of average end-to-end delay in DTLSR and TERP are at almost similar range may due to similarity in selection metric chose in their decision, i.e., shortest path. Thus, in both schemes, the nodes chose among shortest path as their main criteria, thus keeps the value in a consistent range.

VI. CONCLUSION

In this paper, we have proposed an adaptive trust-based routing protocol, called ATRP. Our protocols consider several important issues with regards to multi hop decentralized and randomly distributed wireless sensor nodes in a large scale WSN form. As a network consisting of resource-constraints nodes, energy-aware mechanism is an important factor to be considered. In homogenous network, flooding is the main aspect that consumes energy. In order to provide wider view of the network, we have proposed a hierarchical evaluations of node selection based on direct and indirect trust. By considering group of nodes in route selection, the possibility of chosen best node but having no inheritor can be avoided. In fact, the multi criterion factors considered in the trust metrics in ATRP performs well in decentralized and randomly distributed network. This is proven based on its great performances in terms of lifetime, delay, packet loss and energy consumption.

REFERENCES

[1] S. Tyagi and N. Kumar, "Review: A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 623–645, 2012.

[2] J. Hossein, "An introduction to various basic concepts of clustering techniques on wireless sensor networks," *Int. J. Mobile Netw. Commun. Telematics*, vol. 3, no. 1, pp. 1–17, 2013.

[3] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2000, p. 10.

[4] K. H. Srikanth, "Energy efficient routing protocol for wireless sensor networks," *Int. J. Adv. Comput. Res. Accent Social Welfare Soc.*, vol. 3, no. 2, pp. 95–100, 2013.

[5] H. Abusaimeh and S.-H. Yang, "Dynamic cluster head for lifetime efficiency in WSN," *Int. J. Automat. Comput.*, vol. 6, p. 48, Feb. 2009.

[6] T. Li, M. Fu, L. Xie, and J.-F. Zhang, "Distributed consensus with limited communication data rate," *IEEE Trans. Autom. Control*, vol. 56, no. 2, pp. 279–292, Feb. 2011.

[7] N. A. Khalid and Q. Bai, "Adaptive forwarder selection for distributed wireless sensor networks," in *Multi-agent and Complex Systems*. Singapore: Springer, 2017.

[8] N. A. Khalid, Q. Bai, and A. Al-Anbuky, "An adaptive agent-based partner selection for routing packet in distributed wireless sensor network," in *Proc. IEEE Int. Conf. Agents (ICA)*, Sep. 2016, pp. 37–42.

[9] N. Gautam, W.-I. Lee, and J.-Y. Pyun, "Dynamic clustering and distance aware routing protocol for wireless sensor networks," in *Proc. 6th Symp. Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw.*, 2009, pp. 9–14.

[10] T. P. Le T. J. Norman and W. Vasconcelos, "Adaptive negotiation in managing wireless sensor networks," in *Principles and Practice of Multi-Agent Systems*. Berlin, Germeny: Springer, 2012.

[11] B. An, K. M. Sim, L. G. Tang, C. Y. Miao, Z. Q. Shen, and D. J. Cheng, "Negotiation agents' decision making using Markov chains," in *Rational, Robust, and Secure Negotiations in Multi-Agent Systems*. Springer, 2008.

[12] N. Edalat, C.-K. Tham, and W. Xiao, "An auction-based strategy for distributed task allocation in wireless sensor networks," *Comput. Commun.*, vol. 35, no. 8, pp. 916–928, 2012.

[13] T. Hu, and Y. Fei, "QELAR: A machine-learning-based adaptive routing protocol for energy-efficient and lifetime-extended underwater sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 6, pp. 796–809, Jun. 2010.

[14] S. Gowrishankar, T. G. Basavaraju, D. H. Manjaiah, and S. K. Sarkar, "Issues in wireless sensor networks," in *Proc. World Congr. Eng.*, 2008, pp. 176–187.

[15] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, 2014.

[16] 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 2014.

[17] G. Zhan, W. Shi, and J. Deng, "TARF: A trust-aware routing framework for wireless sensor networks," in *Proc. Eur. Conf. Wireless Sensor Netw.* Singapore: Springer, 2010.

[18] 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.

[19] S. S. Babu, A. Raha, and M. K. Naskar, "A Direct trust dependent link state routing protocol using route trusts for WSNs (DTLSRP)," *Wireless Sensor Netw.*, vol. 3, no. 4, p. 125, 2004.

[20] N. A. Khalid, "Distributed trust-based routing decision making for WSN," Ph.D. dissertation, School Eng., Comput. Math. Sci., Auckland Univ. Technol., Auckland, New Zealand, 2019.

[21] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Auton. Agents Multi-Agent Syst.*, vol. 13, no. 2, pp. 119–154, 2006.

[22] J. Sabater, and C. Sierra, "Regret: A reputation model for gregarious societies," in *Proc. 4th Workshop Deception Fraud Trust Agent Societies*, 2004, pp. 44–56.

[23] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 11, no. 7, pp. 2096–2114, 2013.

[24] B. Sun, and D. Li, "A comprehensive trust-aware routing protocol with multi-attributes for WSNs," *IEEE Access*, vol. 6, pp. 4725–4741, 2017.

[25] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 805–826, 2013.

[26] M. A. Elliott, "Selecting numerical scales for pairwise comparisons," *Rel. Eng. Syst. Saf.*, vol. 95, no. 7, pp. 750–763, 2010.

[27] W. Z. Khan, N. M. Saad, and M. Y. Aalsalem, "An overview of evaluation metrics for routing protocols in wireless sensor networks," in *Proc. 4th Int. Conf. Intell. Adv. Syst.*, Jun. 2012, pp. 588–593.

[28] Y. Al-Obaisat, and R. Braun, "On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management," in *Open Publications of UTS Scholars*. Sydney, NSW, Australia: OPUS, 2007.

[29] F. A. Omondi, *Modeling the Performance of Wireless Sensor Networks*. London, U.K.: MiddleSex University, 2015.

[30] A. K. Gupta, and H. Sadawarti, and A. K. Verma, "Performance analysis of AODV, DSR TORA routing protocols," *Int. J. Eng. Technol.*, vol. 2, no. 2, p. 226, 2010.

[31] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," *IEEE Access*, vol. 1, pp. 35–50, 2013.

[32] J. Duan, D. Yang, S. Zhang, J. Zhao, and M. Gidlund,, "A trust management scheme for industrial wireless sensor networks," in *Proc. 39th Annu. Conf. IEEE Ind. Electron. Soc.*, Nov. 2013, pp. 5576–5581.

NOR AZIMAH KHALID received the bachelor's degree from University Malaya, Malaysia, in 1999, and the M.Sc. degree from the University of Wales, U.K., in 2001. She is currently pursuing the Ph.D. degree with the University of Auckland (AUT), New Zealand. She joined UiTM as a Lecturer, in 2004, then promoted as a Senior Lecturer, in 2012, and since then, she serves with the Department of Computer Technology and Networking.

QUAN BAI received the M.Sc. and Ph.D. degrees from the University of Wollongong, Australia, in 2002 and 2007, respectively. He is currently an Associate Professor with the University of Tasmania, Australia. His current research interests include multiagent systems, data mining, distributed AI, and agent-based modeling for complex systems. He has published more than 100 articles in the above mentioned fields.

ADNAN AL-ANBUKY received the Ph.D. degree from the Institute of Science and Technology, Manchester University, U.K., in 1975. He joined the Auckland University of Technology (AUT), New Zealand, as a Professor, in 2005, and the Head of electrical and electronic engineering. He worked for eight years at Swichtec Ltd., as a Research Specialist, from 1996 to 2004, where he was interacting with the University of Canterbury as an Adjunct Fellow and Technology New Zealand as a Funding Body for conducting industrial research for the company and later, the wider international corporate. He has also a Professor and the Dean of engineering with the Yarmouk University, Jordan, from 1991 to 1995. Over the past few years, he has been invited as a Visiting Professor for number of international institutes. He is currently the Director of the Sensor Network and Smart Environment Research Centre, AUT. His current research interest includes the IoT-based wireless sensor networks targeting cyber-physical intelligence for active stationary and mobile networks. His current focus is on WSN digital twin with the objectives of support for dynamic function and network re-orchestration. He has delivered number of keynote talks, chaired conferences, acted as a member of editorial boards and program committees for good numbers of international conferences, and examined good number of Ph.D. theses. He has also been consulted as a reviewer for number of international funding bodies.