

A secure trust-based protocol for hierarchical routing in wireless sensor network

Maha Al-Sadoon¹, Ahmed Jedidi^{1,2}

¹Department of Computer Engineering, Ahlia University, Manama, Kingdom of Bahrain

²National School of Engineering, Sfax University, Sfax, Tunisia

Article Info

Article history:

Received Apr 23, 2021

Revised Mar 19, 2022

Accepted Mar 30, 2022

Keywords:

Attacks

Cluster head

Cluster-based routing

Trust management

Wireless sensor network

ABSTRACT

Wireless sensor networks (WSNs) became the backbone of the internet of things (IoT). IoT applications are vital and demand specific quality of service (QoS) requirements. In addition, security has become a primary concern to provide secure communication between wireless nodes, with additional challenges related to the node's computational resources. Particular, the design of secure and resource efficient routing protocol is a critical issue in the current deployment of WSNs. Therefore, this paper proposes a novel secure-trust aware routing protocol (ST2A) that provides secure and reliable routing. The proposed protocol establishes communication routes based on calculated trust value in joint with a novel cluster head selection algorithm in the hierarchical routing process. The proposed trust-aware routing algorithm improves the routing security in WSN and optimizes many performance metrics related to WSNs unique characteristics. The results of simulation validate the feasibility of the proposed algorithm for enhancing the network lifetime up to 18% and data delivery by 17% as compared with some state-of-the-art routing algorithms.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Maha Al-Sadoon

Department of Computer Engineering, Ahlia University

Al-Hooraa 310, Gosi Complex, Exhibition Road, P.O. Box 10878, Manama, Kingdom of Bahrain

Email: malsaadoon@ahlia.edu.bh

1. INTRODUCTION

With the rapid development in wireless technologies, sensor nodes (SNs) are used in numerous fields in our daily life in the form of wireless sensor network (WSNs) [1]. WSNs play a vital role in today's real-life applications include monitoring, and tracking physical phenomena surrounding us, also used in the military for surveillance of battlefield [2], [3], others used for sensing public safety in chemical, or biological. Each application has its own quality of service (QoS) requirements. It is recognized as an enabling technology for internet of things (IoT) through collecting, processing, and transmitting a massive amount of data [4], [5]. The SN architecture characterized by the limited performance of a processor, low memory, and limited energy life, which consequently represents a significant barrier to implement an appropriate security system in WSNs. Currently, WSNs has become the pillar of many ecosystem applications, in which security is considered criteria primary concerns due to the high confidentiality of sensors data in some applications. WSNs security has many limitations at many levels. Firstly, the implementation of secure cryptography algorithm faces unusual challenges due to high computational complexity and vulnerability [5]–[7]. Second, as mentioned above, the technology limitation of the SN made the implementation of the traditional security techniques not feasible. As a result, the security mechanisms in WSNs must satisfy the principal requirements and properties such as: confidentiality, integrity, availability, authentication, authorization, privacy, and anonymity [2].

Monitoring and optimizing the communication between the different wireless nodes is important area, which attract research focus. Researchers are mainly concerned with energy consumption problem besides designing optimal algorithms for the routing system to improve the capabilities of WSNs and cope with its limitation. WSNs security based on trust management system is considered as solution to provide secure communication between ad-hoc nodes, through compromising between security levels and limited resources in WSNs [8]. Trust management in routing is used to verify the behavior of the nodes in the WSN that is useful for detecting malicious or faulty node [5]. Trust system has various definitions in research studies based on the tackled scenarios of WSNs. The basic idea is to establish a connection between two neighbor nodes based on trust relation. Indeed, some researchers emphasis on node trust, service trust, or path trust. In general, the trust management system may consider factors related to connectivity, the node process ability, and service availability.

Efficient routing mechanisms that are proposed in the literature is hierarchal routing where the network is divided into clusters. Cluster-based routing protocols are considered as one of the most efficient techniques to minimize energy consumption that may extend the lifetime of WSNs [9]. In the cluster-based network, sink nodes (SNs) are divided to cluster heads (CHs) or cluster members (CMs). SNs send their sensed data to their analogous CHs. CHs aggregate the data and send them to the sink node (SN). Eventually, the end user receives the data from the SN through the internet [3], [9].

This article proposes a new routing technique based on a combination of trust management system and clustering process to improve the security of WSN. Furthermore, explores the history and the state of various connections between nodes to evaluate the trust metrics between different SNs. Based on these trust metrics, we implement the cluster routing to establish secure routes between all the nodes and the sink node. The secure trust-aware routing algorithm (ST2A) compromise between security and QoS were taking into consideration the technical limitations of the SNs.

The rest of the article is structured as follows: the second section briefly presents the different types of attacks in WSN. Also, it provides an overview of related work of routing algorithms based on trust management system and cluster concepts. The third section illustrates the system model and the design assumptions adopted to establish the proposed system. The exhaustive methods for implementing the cluster selection mechanism and the trust system evaluation are provided in the fourth section. The fifth section analyses simulation results by highlighting the improvements achieved by the proposed protocol as compared to state-of-art techniques. Finally, we conclude the paper and highlights future work based on paper contributions.

2. RELATED WORKS

WSNs are highly distributed network deploying thousands of sensors, where the management and monitor of the data are crucial. As a result, the security in WSNs is divided into two vital aspects, which are data security and routing security [10]. This section discusses the related works and research in the area of attack types, trust-aware, and cluster-based routing protocols. Besides, the trust models for secure routing are proposed to cope with the particular attacks and threats present in WSNs.

2.1. Attack types in WSN

The nature of WSNs makes it more susceptible to network attacks such as denial of service (DoS) and eavesdropping due to some causes such as the open medium nature of the wireless channel, lack of centralized monitoring and management, and dynamic network [11]. Moreover, attacks in WSN classified either as internal or external, as presented in Table 1 [4], [12]. In this study, we mainly focus on the trust models' techniques that resist various attacks that may affect data traffics in WSN. Particular, the most objective of our work is to avoid external attacks.

Table 1. Samples of internal and external attacks in WSN

Attacks	Type
Sniffing attack	External
HELLO flood attack	External
DoS attack	External and internal
Wormhole attack	Internal
Stealthy attack	Internal

2.2. Trust routing algorithm in WSN

The trust routing algorithms are proposed to solve the problem of the security issues linked with the different limitation in WSN. This section provides an overview of some well-known security trust routing

models. Trust-aware routing protocol (TARP) that define a secure route to forward messages from the different nodes to the sink based on trust value defined as the confidence level by maintaining a neighborhood description table that provides details about the node neighbors and the quality of the links before interacting with other nodes [13]. The main objective of TARP is to avoid routing through untrustworthy nodes that may end with various resource wastes with no payoff like energy, time, and bandwidth. TARP based on the reputation assessment, and the path reliability evaluation.

Efficient monitoring procedure in reputation system (EMPIRE) aims to minimize the frequency of monitoring activities per node while preserving the ability to detect attacks at a satisfactory level. This reduction implies a saving in the node resources such as energy, memory, and processing. The reputation system in EMPIRE involves three main functions: first monitoring to observe activities of neighbors' nodes which is the most costly in term of resource expense, second rating to evaluate the amount of risk an observer node would offer for the routing operation that may consume a significant amount of resources, third response, where the reputation system is make a decision like avoiding malicious nodes [14].

Trust routing for location-aware sensor networks (TRANS) offers location-centric architecture and performs routing based on trust information rather than hop count to avoid malicious locations and not to affect the data delivery. The TRANS protocol consists of two modules: trust routing module (TRM) that is installed on all the nodes and the insecure location avoidance module (ILAM) is located on the sink node only [15]. During the routing process, the TRANS established secure paths by avoiding misbehaving nodes and identifying insecure location through the implementation of the proposed geographic-based routing protocol [16]. In the early stages of the routing process, every node initializes trust-values for its neighbors and the neighbor sensors steadily forward the messages to trusted neighbors with a nearest geographic position. A node with a trust value below a certain threshold will be treated as a misbehaving node and will be isolated by the sink node.

2.3. Cluster-based routing algorithm in WSN

In addition to the security trust-aware routing protocols, many researchers have proposed different routing approaches, include data-centric or flat routing or attribute routing, hierarchical or cluster-based routing, and location-based routing. The cluster-based routing which is considered in this work - is an energy efficient technique where the SNs perform various duties in WSNs. SNs are arranged into numbers of clusters upon predefined requirements. Each cluster consists of member nodes (MNs) or ordinary nodes (ONs), also a leader node named CH that can be organized into further hierarchical levels. Basically, SNs with sufficient energy will be nominated as CH to process and send data while others with limited energy will action as MNs that sense then send the data to the CH. Hence, this property effects the scalability, extending the network lifetime, reducing the energy, and consequently robustness. The cluster-based routing protocols are classified into three types: grid, block, and chain cluster based [17].

In the cluster-based protocol, the network is split into a number of regions according to specific criteria [18], like the sensing and transmission ranges named cluster. The clustering process starts randomly nominating CHs that control the activities of its associated MNs. MNs will sense, collect, and transmit the data to its CH instead of the base station (BS) which will reduce the communication distance, and consequently the energy consumption, then the CH aggregates the whole data in its cluster and finally transmit the data to the other CHs or the BS [19]. Although these protocols can provide different mechanisms of the clusters' formation and CH selection process, implementing an energy-efficient protocol will growth the WSN lifetime and the network scalability [20].

An example of a cluster-based routing is the low energy adaptive clustering hierarchy (LEACH). It is a self-organizing, probabilistic clustering-based energy efficient routing protocol. That aims to persevere network lifetime, reducing the SN energy depletion of communication with the BS by uniformly distributed the load to all the homogeneous SNs in the WSN [21], [22]. The LEACH process is broken up into rounds; each round is beginning with the setup phase where any SNs maybe selected randomly as a CH for the recent round with a probability ($0 \leq p \leq 1$). When p is smaller than threshold value 5% of SN nominated to be CHs. CH will broadcast their status to other SNs with time slot based on time-division multiple access (TDMA) to allow SN transmitting the sensed data. CH is regularly rotating to preserve battery of a single SN and prevent the selection of a SN with low energy [22]. While in the steady state phase, the SNs sense and transmit the data to belonging CH. Finally, the CH compress, aggregate or fused packet, and then send them to the BS directly.

Power-efficient gathering in sensor information systems (PEGASIS) where the nodes form a chain, which organized by the BS or the SN themselves. With constructing a chain, nodes are assumed to have global knowledge of the networks by employing the greedy algorithm, which ensures that the chain construction process starts at the furthest SN from the BS to guarantee the nearest neighbor, is the next in the SNs chain. The chain is reconstructed when a node in dies and ensures that a particular node is bypassed

[23]. In PEGASIS, SNs are capable of data detection, fusion, and positioning. Therefore, in each round in the data gathering process, a node will receive data from the neighbor node, fuses the data, and retransmit it to the next node in the chain, eventually to the BS. The communications between the nodes are performed through a special token message that is initiated at an arbitrary location by the leader of the network.

3. SYSTEM MODEL

Sink nodes (SNs) are the key components of WSNs, which are distributed according to a specific architecture with the correspondent applications. It is necessary to make these nodes as low-cost and energy efficient to attain high-quality results. Network routing protocols must be designed to achieve fault tolerance in the presence of individual node failure while reducing energy consumption. Given that all sensors in the WSN share the same bandwidth, routing protocols should have the ability to perform collaboration to minimize bandwidth usage. Finally, the sensed data must be transmitted to the sink node, where the end user can access the data. There are many possible models for these WSNs. In this section, we present the adopted node and network models in this study. The WSNs components used in this research has the following features:

Firstly, we assume that all the SNs are homogenous in terms of communication, processing, and storage capabilities. Furthermore, each sensor is initiated by the same amount of energy noted E_i . The base station (sink) has fixed positioned, far from the sensor members, which represents a gateway to other networks. Moreover, SNs are randomly distributed and can obtain information related to their geographical location and their neighbor's locations, according to the localization techniques as proposed in [24]. Also, each SN is assigned a unique identification number, sensing range denoted by r , and communication range R where $R = 2r$.

The SN plays two roles, either as a receiver or as a transmitter in which each role has an energy model. Equation (1) and (2) present the energy model adopted by [11] and [19] where both free space and multi-path fading channels are employed according to the distance between the transmitter node i and the receiver node j and defined as $D_{(i \leftrightarrow j)}$. If the distance is higher than or equal to the threshold value, which is stated by d_0 , then the multi-path mp model is used. Otherwise, the free space fs model is considered. The amplification energy for the shortest distance, which is the free space model defined as θ_{fs} and for the longest distance, which is the multi-path model defined as θ_{mp} . This energy model considers both channel models of the free space with $D_{(i \leftrightarrow j)}^2$ power loss while multi-path fading with $D_{(i \leftrightarrow j)}^4$ power loss whereas δ_t and δ_r are the energy dissipated in transmitting and receiving one bit correspondingly. Therefore, to send a β -bit data packet from node i to node j the consumption energy is calculated by (1) while the consumption energy for the receiving β bit data packet by node j is given by (2):

$$E_t(i, j) = \begin{cases} (\delta_t + \theta_{fs} D_{(i \leftrightarrow j)}^2) \beta, & D_{(i \leftrightarrow j)} < d_0 \\ (\delta_t + \theta_{mp} D_{(i \leftrightarrow j)}^4) \beta, & otherwise \end{cases} \quad (1)$$

where $d_0 = \sqrt{\theta_{fs}/\theta_{mp}}$

$$E_r(j) = \delta_r \beta \quad (2)$$

Secondly, SNs are organized as a hierarchical structure and grouped into several clusters, i.e., stages. Each SN can take two states either CH or cluster member (CM). Initially, all the nodes in WSN are assigned a CM state, and transit to the different CH's states according to the proposed select cluster mechanism (SCM), which be explained in detail in the next section. Also, we assume that each stage in the network has at least one CH node controlling the CMs. Finally, the connection between two adjacent nodes ensures the successful delivery of different information. The nodes periodically alter information such as energy, localization, and connection state.

The network architecture used in this work is illustrated in Figure. 1. We assume that all nodes located between d and $d + r$ belong to the same stage j of the network as formulated in (3). Therefore, the network model incorporated in this study is composed of M SNs distributed through N stages, and a sink node is located in the first stage. Each node is capable to communicating with other nodes in the same stage, backward stage, or forward stage, restricted by the node position and bounded by the transmission area R .

$$N_i^{localization} \in [d_j, d_j + r] \xleftrightarrow{stage\ j} N_{i,j}, j \in [2, N] \quad (3)$$

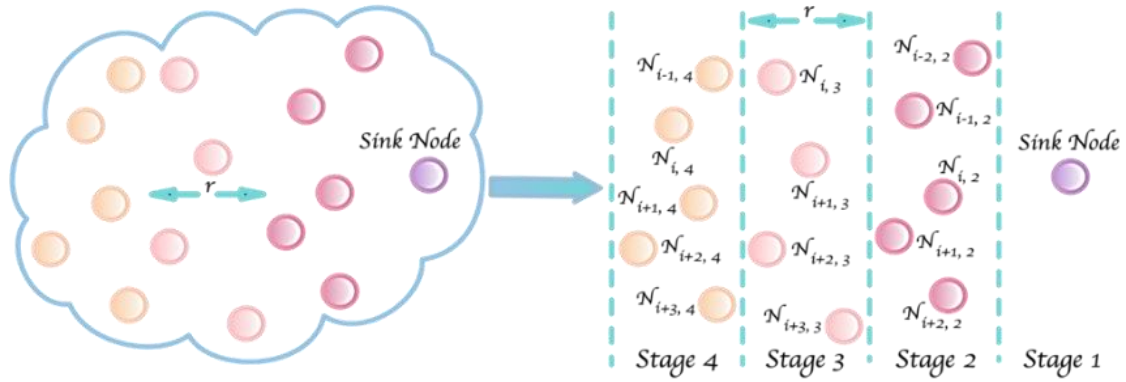


Figure 1. Wireless sensor network model

4. PROPOSED ALGORITHM FOR THE TRUST ROUTING SYSTEM

Security in WSNs is critical issues to achieve the efficiency and confidentiality of data transfer. The secure routing algorithm is essential to guarantee the network functionality in the face of malicious or other attacks and to balance the traffic load, which consequently improves the security throughout the whole network [22] and [25]. In this section, we present our proposed routing algorithm to improve the security and the performance of WSNs. The ST2A is based on two key concepts: the trust management system and the cluster selection system. We define the trust value as a combination and balance of many network parameters as discussed later. The implemented clustering mechanism is also detailed in the following subsections.

4.1. Selection cluster mechanism

In a cluster system we suggested two types of node states first, the CH and second the CM. The transition between the states passed through a particular mechanism, where all nodes in WSNs begin as CM state and according to the selection cluster mechanism (SCM) transit to another state. Figure 2 shows the four suggested states, with its features and privileged connections to establish the route from the source node to the sink node.

4.2. Trust system evaluation

Trust is significant to constructive interpersonal relationships in different settings since it is central to form a collaborative relationship, and enhance the interaction with others they can trust, based on a face-to-face assessment or societal reputation. Because the trust is considered so vital, the researchers have studied it extensively for a long time, beginning with the social sciences that survey the trust between humans to the effects of trust in economic transactions. Along with trust notion, comes of reputation, so trust is derived from the reputation. The reputation itself is built over time, according to the entity’s history of behavior that may reflect a positive or negative assessment. The concepts of trust and reputation management have been extensively adopted in large sectors such as e-commerce, web services, ad-hoc networks, social network, and so on [13]. In this context, the researchers attempt to model the security problems in WSN, as highlighted in subsection 2.

In this study, the key parameter of the trust concept is the history of an active connection between two adjacent nodes. For each node $N_{i,j}$ (i the ID of the node in the j stage) we associate a trust history table ($THT_{i,j}$) which presents the related information for all nodes connected to $N_{i,j}$. We define $N_{k,l}$ as the different nodes connected to $N_{i,j}$ which $l \in \{j, j + 1\}$ and $k \in [1, z]$. The THT contains the number of active connections, energy consumption, location, and node state. Based on parameters as mentioned earlier, we define the trust value $Tv_{N_{k,l}}^{N_{i,j}}$ corresponding to each couple of nodes according to (5). Note that, $N_{i,j} \leftrightarrow N_{k,l}$, where $N_{k,l}$ presents the node connected with $N_{i,j}$ and w is the number of nodes connected to $N_{i,j}$.

$$Tv_{N_{k,l}}^{N_{i,j}} = NC^{(LO_{k,l}-1)} + \sum_{m \in \{j, j+1\}, n \in \{[1, z] \setminus k\}} \left(EC_{k,l}^{LO_{k,l}} - \frac{EC_{m,n}^{LO_{m,n}}}{w} \right) + SN_{i,j} * SN_{k,l}^{LO} \quad (4)$$

The trust value balances between three main parameters: first, the number of active connections, such that the nodes located in the next stage are given more than the nodes located in the same stage. Second, the residual energy EC , defined as the difference between the energy of the candidate node and the average of

the rest of the energy nodes. Third, the state node SN , which is produced according to the states of node couples. We note that the location of the candidate node has a direct impact on the different parts of Tv formula in (4). As a result, the location of the node has a highly significant impact on the trust value, which determines the route from the source node to the sink node.

To determine the number connection NC in the THT, each node $N_{i,j}$ at stage j tries to connect with the nodes in the transmission area R and which are located in the same or next stages as shown in Figure 3. Meanwhile, $N_{i,j}$ collects the different information from the candidate nodes as mentioned above and defines NC according to the connection history algorithm (CHA) presented in Algorithm 1. For each iteration, the $N_{i,j}$ examines the active connection with different nodes at its area R . If the connection is correct (i.e., a positive acknowledgment received), and the node is located in the next stage, the value of NC will be incremented by two. Otherwise, if the node is located in the same stage, NC will be incremented by 1. If the connection fails, the NC will be decremented by 1.

Algorithm 1. Pseudocode of connection history algorithm

Input: nodeID, node stage, node range transmission

Output: find the number of connected nodes associated with each node in WSN.

```

For  $i \leftarrow 1$  To  $M$  //  $M$  is the total number of nodes in the WSN
     $N\_Cur \leftarrow N(i)$  //  $N(i)$  is the current node ID
     $NStage\_Cur \leftarrow NStage(i)$  //  $NStage(i)$  is the stage of the current node
    For  $j \leftarrow 1$  To  $Z \subseteq M$  //  $Z$  is the total number of nodes within the transmission range  $R$ 
         $N\_Can \leftarrow N(j)$  //  $N(j)$  is the candidate node ID
         $NStage\_Can \leftarrow NStage(j)$  //  $NStage(j)$  is the stage of the candidate node
        If  $NStage\_Cur = NStage\_Can + 1$  Then //determine the priority of the connected stage
             $NC \leftarrow NC + 2$ 
        Else If  $NStage\_Cur = NStage\_Can$  Then
             $NC \leftarrow NC + 1$ 
        End If
    End For
End For
    
```

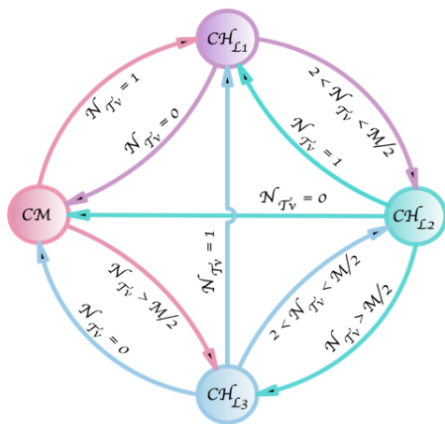


Figure 2. The state diagram of the selection cluster mechanism

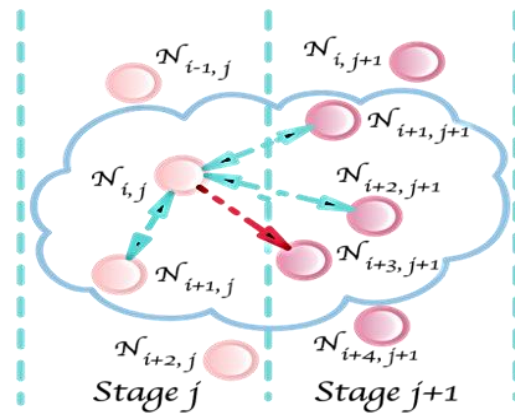


Figure 3. Connection mode between sensor nodes

4.3. Secure trust-aware algorithm

In spite of the numerous researches and the significant growth in recent years, many routing protocols in WSN still face several issues that need to be resolved. The main goal of the routing protocols includes data communication while maximizing the network lifetime, packet delivery, and minimizing energy consumption. These goals can be achieved by employing an efficient path selection algorithm. In this section, the proposed algorithm, which is a hybrid cluster, and trust value-based routing, is described in detail. The ST2A balances between security in data transfer and the different above parameters.

The main idea of TS2A is to combine between the trust value and the state of the node to define a secure and efficient route from a source node to a sink node. Furthermore, the status of connections between nodes has a direct impact on the Tv and the cluster state. Likewise, the location of node intervenes directly to these parameters. Consequently, TS2A has the following metrics: node location, node status, and trust value, as shown in pseudocode algorithm 2.

Algorithm 2. Pseudocode to determine the connection between the nodes in WSN

Input: nodeID, node state, node stage, node range transmission, calculated trust value of the node

Output: find the connectivity between the nodes.

```

1. For  $i \leftarrow 1$  To  $M$  //  $M$  is the total number of nodes in the WSN
2.    $N\_Cur \leftarrow N(i)$  //  $N(i)$  is the current node ID
3.    $NStage\_Cur \leftarrow NStage(i)$  //  $NStage(i)$  is the stage of the current node
4.   For  $j \leftarrow 1$  To  $Z \subseteq M$  //  $Z$  is the total number of nodes within the transmission range
5.     Do While  $i \neq j$ 
6.       For  $k \leftarrow 1$  To  $Z$ 
7.          $N\_Can \leftarrow N(K)$  //  $N(k)$  is the candidate node ID
8.          $NStage\_Can \leftarrow NStage(k)$  //  $NStage(k)$  is the stage of the candidate node
9.          $cS3 \leftarrow 0$ ,  $cS2 \leftarrow 0$ ,  $cS1 \leftarrow 0$  //  $cS$  is the initial count of each state
10.        Select Case  $S$  // determine the maximum trust value of each state,  $S$  is the cluster node level, i.e., state (1, 2, or 3)
11.          Case 3
12.             $cS3 \leftarrow cS3 + 1$ 
13.            If  $cS3 = 1$  Then
14.               $maxTv \leftarrow NTv(k)$  //  $NTv$  is the trust value of each node which calculated using (4)
15.            Else
16.              If  $maxTv < NTv(k)$  Then
17.                 $maxTv \leftarrow NTv(k)$ 
18.              End If
19.            End If
20.          Case 2
21.             $cS2 \leftarrow cS2 + 1$ 
22.            If  $cS2 = 1$  Then
23.               $maxTv \leftarrow NTv(k)$ 
24.            Else
25.              If  $maxTv < NTv(k)$  Then
26.                 $maxTv \leftarrow NTv(k)$ 
27.              End If
28.            End If
29.          Case 1
30.             $cS1 \leftarrow cS1 + 1$ 
31.            If  $cS1 = 1$  Then
32.               $maxTv \leftarrow NTv(k)$ 
33.            Else
34.              If  $maxTv < NTv(k)$  Then
35.                 $maxTv \leftarrow NTv(k)$ 
36.              End If
37.            End If
38.          End Select
39.        End For
40.      If  $NStage\_Cur = NStage\_Can$  Then // determine the priority of the connected stage
41.         $prior \leftarrow normal$ 
42.      Else If  $NStage\_Cur = NStage\_Can + 1$  Then
43.         $prior \leftarrow high$ 
44.      End If
45.      If  $cS3 \geq 1$  Then // establish the link between the source node and the candidate node with the range transmission
46.        If  $prior = high$  Then
47.           $N\_Cur \leftrightarrow N\_Can$ 
48.        Else
49.           $N\_Cur \leftrightarrow N\_Can$ 
50.        End If
51.      Else If  $cS2 \geq 1$  Then
52.        If  $prior = high$  Then
53.           $N\_Cur \leftrightarrow N\_Can$ 
54.        Else
55.           $N\_Cur \leftrightarrow N\_Can$ 
56.        End If
57.      Else If  $cS1 \geq 1$  Then
58.        If  $prior = high$  Then
59.           $N\_Cur \leftrightarrow N\_Can$ 
60.        Else
61.           $N\_Cur \leftrightarrow N\_Can$ 
62.        End If
63.      End If

```

```

64.   End While
65.   End For
66.   End For

```

The proposed routing algorithm is considering various routing metrics parameters. In this discussion, we assume that M is the set of all homogeneous nodes in WSN, initially all nodes have equal capabilities such as processing capacity, battery life, sensing range, and transmission range. Each node initiating a connection (source node) is responsible for monitoring the behavior of its neighbor nodes (target nodes) and evaluating their trust value. Once a source node $N_i \in M$ establishes a connection with its neighbor node within its transmission range R , the following process is implemented:

- The nodes connection is based on two criteria: First criterion is the trust value Tv that has been calculated for each node using (4), which then is stored in the updated trust value history table. The node N_i is the evaluating device, and node N_k is the evaluated one. If the node N_k has the maximum trust value $maxTv$, that recommend her to has a higher priority to obtaining the connection with trustworthy node. The second criterion is the node state. Each node has a specific state value associated with it based on a predefined threshold, in which it belongs to one of the three states S : state 1, state 2, or state 3. State 3 has the highest priority, followed by state 2, while state 1 has the least priority to attain the connection.
- After the above two processes are accomplished, further construction of the routing is proceeded to obtain an optimal path. When a source node plan to transmit packets to a destination node (sink) via a multi-hop connection, the selection of the next candidate node is based on employing a priority to evaluate the most applicable SNs. There are two different stages within a specific sensing range, which are the current stage with moderate priority and next stage with high priority, in addition to the previous stage with low priority. Each node can gain a link to a node in the same stage or the next stage only in all cases. A rout is considered to be efficient when the link connection is defined from node to another located in the next stage.

5. SIMULATION RESULTS AND DISCUSSION

The experimental results of the proposed algorithm TS2A are presented in this section. The simulation is performed using MATLAB with the simulation parameters shown in Table 2. Moreover, we benchmark the results of the proposed algorithm with two state-of-the-art algorithms in the literature, i.e., LEACH for the cluster-based algorithm and EMPIRE for the trust-based algorithm. To understand the function of the proposed system, we begin by testing and evaluating the behavior of the cluster mechanism. Furthermore, we simulated a network composed of 600 homogenous SNs in which we investigated the state of each node as function the number of rounds, as shown in Figure 4.

Table 2. Simulation parameters

Parameter definition	Symbol	Value
Sensor deployment area (Network size)	-	100×100 m
Number of nodes	M	600
Sink position	$Sink$	(1, 1)
Communication range	R	10 m
Sensing range	r	5 m
Initial energy	E_i	0.5 Joules
Tx or Rx Transceiver energy	$\delta_t = \delta_r$	50 nJ/bit
Free space amplifier energy	θ_{fs}	10 pJ/bit/m ²
Multi-path amplifier energy	θ_{mp}	0.0013 pJ/bit/m ⁴
Data packet size	β	500 bits
Control message size	C	100 bits

The investigation of the nodes state indicates that the number of nodes that adopt CH_{L1} state is significant compared to the CH_{L2} and CH_{L3} states at the start and the end of the simulation. In fact, at the beginning of the simulation time, most of the SNs still have not built the right connection links with the other nodes, which implies that the CH_{L1} state is more adopted. Likewise, the same state CH_{L1} takes place at the end of the simulation time because the number of dead SNs is increased. Otherwise, as the simulation time progresses, we notice that the state of the CH_{L2} and CH_{L3} take place in a balanced way. Mainly, a SN N_j swaps between CH_{L2} and CH_{L3} during the simulation between 1,000 rounds and 3,500 rounds because of the number of the nodes connected to N_j is between $\left[2 \frac{M}{2}\right]$ and $\left[\frac{M}{2} M\right]$. Also, we observed that the rate of the various states is almost the same in the middle of simulation time. However, this situation changes at the

beginning and the end of the simulation. As a result, the balance between the different states increases the network lifetime. Moreover, the SNs swap between the active and passive roles in which it forwards data in the active situation and standby for the passive one. To validate the performance of the proposed system, we evaluated various measures and compared them with benchmarked algorithms. Precisely, we investigated the lifetime, energy consumption, and data delivery for the WSN.

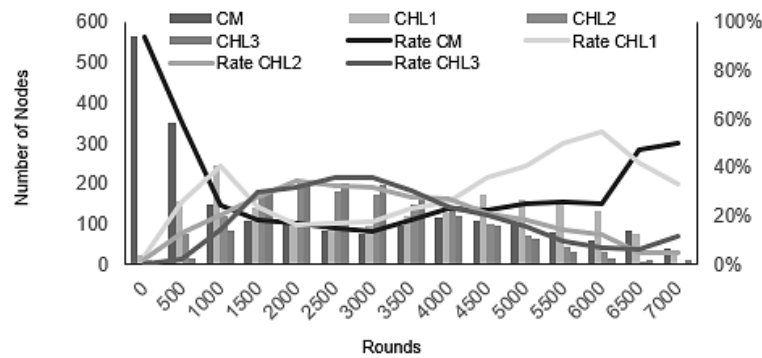


Figure 4. Cluster states behaviors

First, we evaluate and discuss the network lifetime, as shown in Figure 5. We noticed that the network lifetime for the ST2A outperformed the LEACH and EMPIRE by more than 18%. Furthermore, the number of the dead SNs is higher for LEACH and EMPIRE as compared to ST2A algorithm. This observation is valid when the number of rounds starts from 1500, where the proposed algorithm has the flexibility to swap and balance the node states according to the trust value. ST2A allows the SN to swap between the various states then SN balances between the function of forwarding data and the role of sending its data. As a result, the residual energy of the SNs decreases slightly, then the sensor lifetimes increase, which it has a direct impact on increasing the network lifetime.

Second, we investigated the impact of the proposed algorithm on the residual energy as function the number of rounds, as shown in Figure 6. We observed that ST2A improves the residual energy compare other algorithms by up to 21%. Precisely, ST2A has the highest impact on the residual energy between 1,500 and 3,500 rounds. Moreover, the swapping between the various cluster states allows the SN to save their residual energy by reducing the workload of forwarding data in the routing function. The balance of the workload for the different SNs in the network improves the average residual energy for the overall network.

Third, Figure 7 focuses on the evaluation of the data delivery or the performance of the network function. In objective to measure this parameter, we tested the proposed algorithm for three scenarios. Indeed, we select these scenarios to test and evaluate the performance of ST2A in normal and extremes conditions according to the energy and the circulate data.

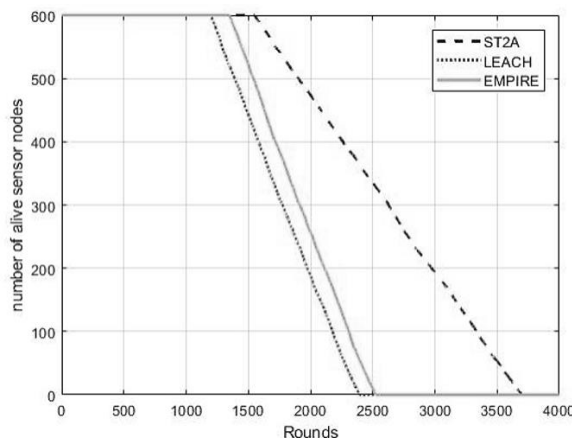


Figure 5. Number of alive sensor nodes

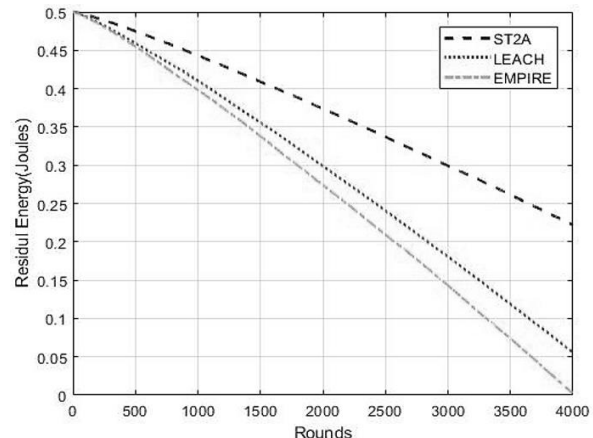


Figure 6. The average of the residual energy

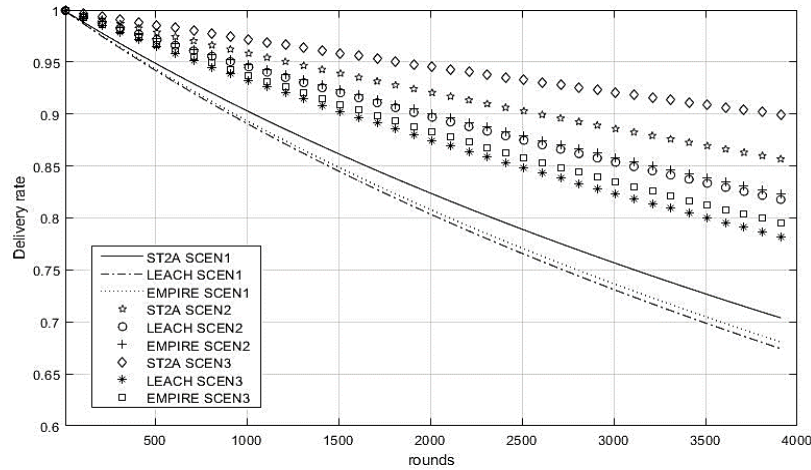


Figure 7. The performance of the proposed algorithm ST2A

First, we injected 60000 data packets for all network composed of 600 SNs in which each SN has 1,000 packets to send, and all nodes begin with the same initial energy. Second, we distribute 60,000 data packets to 300 SNs according to a linear way. Moreover, we began the simulation by 100 packets for the nodes in the first stage, then the number of packets is incremented by 50 for each node. Finally, the third scenario allocates 60,000 data packets for 300 SNs randomly distributed, which the network has 300 SNs start running with half of the initial energy randomly distributed. We noticed that the ST2A improved the data delivery with more than 17% compared to LEACH and EMPIRE. Moreover, the impact of the ST2A is clearly emphasized in the second and third scenarios in which the energy and the workload are required. Moreover, we compared the packet loss for the proposed algorithm as function the size of the network. We observed that the rate of the packet loss decreases compares to LEACH and EMPIRE, as shown in Figure 8. Indeed, ST2A improves the rate of the data delivery when the size of the network increases according to the workload balance and cluster mechanism, especially when the density of the SNs is large.

To evaluate ST2A algorithm performance in terms of security, we simulated a network composed of 600 SNs, in which five nodes create a DoS attack, and five others create a stealthy attack. We observed that the ST2A discovers these attacks with 85% success rate. Particularly, ST2A secure the network from the external attacks because it uses a trust routing system.

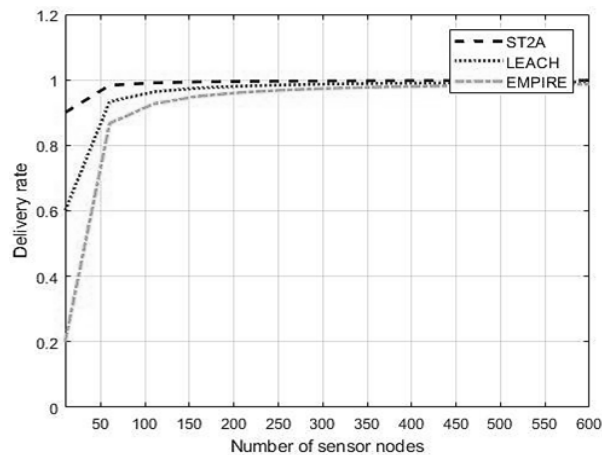


Figure 8. The data delivery rate vs size of the network

6. CONCLUSION

As wireless sensor network plays an essential role in most of the applications related environment monitoring, which is under the umbrella of the internet of things, the need for security in that become inevitable and vital. However, WSN faces a challenge according to the inherent characteristics that incur

constraints to the SNs which present a significant barrier for the implementation of traditional routing algorithms. Based on this fact, finding an adequate routing algorithm is necessary. In this paper, the proposed ST2A goals are categorized into two main types. First, improve the energy consumption by adopting the cluster head selection, which consequently extends the lifetime of WSN. Second, increase the level of security by implement trust management system that is capable of establishing connections between SNs throughout WSN based on a combination of several features such as connection history, residual energy, node location, and state. Moreover, the most well-known and latest routing algorithms (i.e., LEACH and EMPIRE) based on their features are reviewed and compared in each goal category. When compared ST2A with others, significant improvements have been observed. The proposed algorithm maximized the nodes lifetime by 18% in comparison with LEACH. Therefore, a scalable solution which can perform a hybrid algorithm by considering multi-objective of QoS requirements is seriously required in WSNs.

The future scope of this paper is to extend the proposed algorithm into heterogeneous WSN and incorporate more parameters such as SNs mobility. Another trend could be customizing the proposed algorithm based on the complexity of IoT applications. We believe that time-critical applications such as healthcare requires a high-security level and quick actions, while others can be less restrictive such as logistic. Accordingly, the proposed algorithm needs to be modified.

REFERENCES





- [1] D. M. Mena, I. Papapanagiotou, and B. Yang, "Internet of things: survey on security," *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 162–182, May 2018, doi: 10.1080/19393555.2018.1458258.
- [2] M. A. Khan and M. Khan, "A review on security attacks and solution in wireless sensor networks," *American Journal of Computer Science and Information Technology*, vol. 7, no. 1, 2019.
- [3] A. Jedidi and A. Mohammad, "History trust routing algorithm to improve efficiency and security in wireless sensor network," in *2017 14th International Multi-Conference on Systems, Signals and Devices (SSD)*, Mar. 2017, pp. 750–754, doi: 10.1109/SSD.2017.8166988.
- [4] I. Souissi, N. Ben Azzouna, and L. Ben Said, "A multi-level study of information trust models in WSN-assisted IoT," *Computer Networks*, vol. 151, pp. 12–30, Mar. 2019, doi: 10.1016/j.comnet.2019.01.010.
- [5] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards internet of things," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2017, pp. 1–6, doi: 10.1109/CCWC.2017.7868374.
- [6] A. Alromih, M. Al-Rodhaan, and Y. Tian, "A randomized watermarking technique for detecting malicious data injection attacks in heterogeneous wireless sensor networks for internet of things applications," *Sensors*, vol. 18, no. 12, Dec. 2018, doi: 10.3390/s18124346.
- [7] I. Vaccari, E. Cambiaso, and M. Aiello, "Evaluating security of low-power internet of things networks," *International Journal of Computing and Digital Systems*, vol. 8, no. 2, pp. 101–114, Jul. 2019, doi: 10.12785/ijcds/080202.
- [8] M. M. Afsar and M.-H. Tayarani-N, "Clustering in sensor networks: a literature survey," *Journal of Network and Computer Applications*, vol. 46, pp. 198–226, Nov. 2014, doi: 10.1016/j.jnca.2014.09.005.
- [9] A. Yasin and K. Sabaneh, "Enhancing wireless sensor network security using artificial neural network based trust model," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 9, 2016, doi: 10.14569/IJACSA.2016.070932.
- [10] R. T. Merlin and R. Ravi, "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET," *Wireless Personal Communications*, vol. 104, no. 4, pp. 1599–1636, Feb. 2019, doi: 10.1007/s11277-019-06120-8.
- [11] V. Hiremani, "Secure mechanism for wireless sensor networks - a review," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 1, no. 12, pp. 915–918, 2013.
- [12] M. M. Alqhatani and M. G. M. Mostafa, "Trust modeling in wireless sensor networks: state of the art," *Journal of Information Security and Cybercrimes Research*, 2018, doi: 10.26735/16587790.2018.007.
- [13] I. Maarouf, U. Baroudi, and A. R. Naseer, "Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks," *IET Communications*, vol. 3, no. 5, pp. 846–858, 2009, doi: 10.1049/iet-com.2008.0324.
- [14] T. Zahariadis *et al.*, "Design and implementation of a trust-aware routing protocol for large WSNs," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, pp. 52–68, Jul. 2010, doi: 10.5121/ijnsa.2010.2304.
- [15] P. R. Vamsi and K. Kant, "Trust and location-aware routing protocol for wireless sensor networks," *IETE Journal of Research*, vol. 62, no. 5, pp. 634–644, Sep. 2016, doi: 10.1080/03772063.2016.1147389.
- [16] S. P. Singh and S. C. Sharma, "A survey on cluster based routing protocols in wireless sensor networks," *Procedia Computer Science*, vol. 45, no. C, pp. 687–695, 2015, doi: 10.1016/j.procs.2015.03.133.
- [17] S. Mahajan and P. K. Dhiman, "Clustering in wireless sensor networks: a review," *International Journal of Advanced Research in Computer Science*, vol. 7, no. 3, pp. 198–201, Oct. 2016.
- [18] K. Cengiz and T. Dag, "Energy aware multi-hop routing protocol for WSNs," *IEEE Access*, vol. 6, pp. 2622–2633, 2018, doi: 10.1109/ACCESS.2017.2784542.
- [19] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: a top-down survey," *Computer Networks*, vol. 67, pp. 104–122, Jul. 2014, doi: 10.1016/j.comnet.2014.03.027.
- [20] P. Vyas and M. Chouhan, "Survey on clustering techniques in wireless sensor network," *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 5, no. 5, pp. 6614–6619, 2014.
- [21] N. R. Wankhade and D. N. Choudhari, "Novel energy efficient election based routing algorithm for wireless sensor network," *Procedia Computer Science*, vol. 79, pp. 772–780, 2016, doi: 10.1016/j.procs.2016.03.101.
- [22] H. Singh and D. Singh, "Taxonomy of routing protocols in wireless sensor networks: a survey," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Dec. 2016, pp. 822–830, doi: 10.1109/IC3I.2016.7918796.
- [23] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," in *Conference Record / IEEE Global Telecommunications Conference*, 2001, vol. 5, pp. 2926–2931, doi: 10.1109/glocom.2001.965964.
- [24] M. Z. Hasan, H. Al-Rizzo, and F. Al-Turjman, "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 3, pp. 1424–1456, 2017, doi:

10.1109/COMST.2017.2661201.





- [25] P. Lou, L. Yuan, J. Hu, J. Yan, and J. Fu, "A comprehensive assessment approach to evaluate the trustworthiness of manufacturing services in cloud manufacturing environment," *IEEE Access*, vol. 6, pp. 30819–30828, 2018, doi: 10.1109/ACCESS.2018.2837664.

BIOGRAPHIES OF AUTHORS



Maha Ebrahim Al-Sadoon     she received the B.S. and M.S. degrees in Information Technology and Computer Science from Ahlia University, Manama, Bahrain, in 2006 and 2010, respectively. She is currently working toward the Ph.D. degree in the School of Electronic and Computer Engineering, Brunel University, London. She was a Research Assistant with the Computer Engineering Department, Ahlia University. Since 2010, she has been a lecturer at the same University. Her research interests include the artificial intelligent (AI), genetic algorithms (GA), internet of things (IoT), wireless sensor network (WSN), and big data. She can be contacted at email: malsaadoon@ahlia.edu.bh.



Ahmed Jedidi     received the B.S. degree in electrical engineering from National Engineering School of Sfax University, Sfax, Tunisia, in 2005 and the M.S. and Ph.D. degree in computer engineering from National Engineering School of Sfax University, Sfax, Tunisia, in 2006 and 2012, respectively. From 2006 to 2009, he was a Contractual Assistant with both the Higher Institute of Applied Sciences and Technology, Computer Engineering Department, Sousse University and Institute of Computer Science and Mathematics, Computer Engineering Department, Monastir University. Since 2009, he has been an Assistant Telecommunication with the National Engineering School, Communication and Network Engineering Department, Gabes University. Then he has been an Assistant Professor with the same University in the High Institute of Computer science and Multimedia, Telecommunication Engineering Department in 2012. Later on, from 2013 to 2015 he joined Technical College of Computer Engineering Department, Dammam, Saudi Arabia. Where he is currently an Assistant Professor in Computer Engineering Department, Ahlia University, Bahrain, also he is the Chairperson of that Department. He is also with the Computer and Embedded Systems laboratory, Sfax University, Tunisia. His research interests include the detection, localization, and estimation of crosstalk in all-optical networks (AONs), the optical networks communication, the reliability of multiprocessor operating systems, the embedded system performance and Wireless sensor network. She can be contacted at email: ajedidi@ahlia.edu.bh.