

Modified Particle Swarm Optimization in Wireless Sensor Network for Clustering and Routing



R. Vijaya Prabhu, S. Anslam sibi, and R. Priscilla

Abstract Wireless sensor networks are composed of sensor nodes and are being deployed in many applications, where security is deemed critical. In WSN, the data collected at any node is forwarded to any designated sink node either through single or multiple hops. Due to the weaker nature and intrinsic, they are easily brought down by external security attacks. The routing plays a vital role in forwarding data from one node to another. Optimal route discovery in WSN is often problematic due to several factors like drain of energy in the node and so on. The residual energy of nodes located near the sink area has the high probability of getting drained out sooner than nodes in other areas. The proposed research addresses this issue through an energy-efficient clustering technique and trustable routing protocol specifically designed for WSNs that minimize the energy consumed by the nodes at the sink area. In this work, a novel clustering algorithm based on modified particle swarm optimization (MPSO) technique had been proposed to form clusters that engage in selecting the cluster heads at the sink coverage area and account for devising a solution to the energy hole problem. Also an energy trust system (ETS) for WSNs had been formulated in the proposed research for effectively detecting the Sybil attacks. Multi-level detection based on identity and position verification is carried by the proposed ETS. Cluster-based trust-aware secure routing had been performed in the proposed research that successfully detects the available active nodes prior to forwarding any data and establishes alternate routes, if need arises. The main aim of the proposed research is to preserve energy of nodes and improvise the security of data while routing from source to sink nodes.

Keywords WSN · Energy conservation · Energy hole problem · Sybil attacks · Energy trust system · Clustering · Modified particle swarm optimization algorithm

R. Vijaya Prabhu (✉) · S. Anslam sibi · R. Priscilla
St. Joseph's Institute of Technology, Chennai, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021
R. J. Kannan et al. (eds.), *International Virtual Conference on Industry 4.0*,
Lecture Notes in Electrical Engineering 355,
https://doi.org/10.1007/978-981-16-1244-2_30

347

1 Introduction

The wireless sensor network is advancing in recent years. The sensor devices are mostly used as input devices to detect physical or environment conditions. In this, node to node data transmission is done by calculating base station distance using various algorithms.

A wireless sensor network is composed of numerous tiny sensors that monitor and track information about the environment in which they are deployed. The aggregated information is transmitted through wireless links to any designated sink node. Data is relayed through several intermediate nodes across a gateway towards the destination node like a wireless Ethernet.

2 Literature Survey

2.1 Routing Techniques

Souihli et al. [1] had proposed a novel a load balancing mechanism that could be applied in MANET using shortest path routing protocols. Distribution of maximum load is observed at the centre of the network, and accordingly, the proposed load balancing schemes drive the traffic or the observed load from the centre of the network. Based on the characteristics of routing protocol, the central node is designated as proactive or reactive. In reactive types, the nodes are characterized according to their centrality that is based on the size of their routing tables. In proactive types, the centrality of a node is fixed based on its multi-point relay selector list. The proposed load balancing schemes provide efficient load distribution, end-to-end delay and packet delivery fraction. The proactive feature in the proposed schemes effectively identifies the nodes that are congested and overloaded and relieves them. The authors had not taken into account of the performance of their schemes under non-uniform node distributions.

Protecting the privacy of the sink nodes in WSN is highly challenging. The sink nodes are highly vulnerable as they can easily fall prey to adversaries who can eavesdrop on the packets to identify its destination. The sink node privacy issue had been addressed by Long et al. [2] who had proposed a ring-based routing (RBR) technique. In the RBR technique, the authors had introduced the concept of multiple rings and multiple routing lines. Data is not directly transmitted to the sink node instead to the nearest routing ring. Data transmission takes place through routing rings that are relayed by further rings through routing lines till it reaches the destination. The count of anonymous sink nodes is kept equal to the number of network nodes. The proposed RBR technique is highly scalable and increases the network lifetime and accounts for high energy efficiency.

Lee et al. [3] had analysed the adhoc networks and had proposed the split multi-path routing (SMR) protocol. The proposed SMR protocol functions as on-demand

protocol that creates maximum number of disjoint routes. Each session of data transmission comprises of two routes, namely the shortest delay route and maximally disjoint shortest delay route. These maximum disjoint routes are designed with the idea of avoiding routes that may be congested to efficiently utilize the network resources. In adhoc networks, the presence of multiple paths helps in overcoming disconnected routes where source can choose any available route without the necessity of route recovery. The proposed protocol introduces end-to-end delay whenever routes are disconnected and consumes more energy during such occurrences.

Hu et al. [4] had proposed a technique that brings a balance between the quality of detecting the target and the lifetime of WSN. The authors had proposed an intelligent adjustable sensing frequency for mobile target detection based on the monitor quality optimization. In the proposed technique, the target is monitored using two schemes, namely target detection with sensing frequency K (TDSFK) and target detection with adjustable sensing frequency (TDASF). The former technique senses the frequency increase from 1 to K , and the latter technique adjusts the sensing frequency on nodes having residual energy. The two techniques are adaptable for networks containing static sinks and are not suited for networks with mobile sinks.

Zhang et al. [5] had proposed a dynamic sensing technique that addresses the routing issues for maximizing the utilization of rechargeable sensor networks. The authors had proposed a balanced efficient energy allocation scheme (BEAS) that manages the energy utilization in sensor nodes and makes the entire process as smooth as possible. In the proposed technique, the optimal sensing rate and routing control had been accounted through a distributed sensing rate and routing control (DSR2C) algorithm. The cost expended in managing the energy allocation and controlling the topology is very high in the proposed technique.

2.2 Cluster Formation Techniques

Li et al. [6] had analysed the WSN and proposed that resource efficiency and dependability of a trust system are required for securing data. Present trust systems are generating too much overhead and possess low dependability, hence not suitable for enforcing high security. The authors had proposed a lightweight and dependable trust system (LDTS) for WSNs that employ clustering algorithms. Energy preservation is brought in using a lightweight trust decision-making technique that operates based on identities of nodes in the WSN clusters. The effect of malicious nodes is negated, and system efficiency is improved by cancelling of feedback between the individual cluster members or cluster heads. Since huge data is forwarded by the cluster heads, a dependability-enhanced trust evaluating approach had been implemented at the cluster heads for cooperation purposes. It is huge improvement when compared to traditional techniques that fix weights subjectively. When compared with existing trust systems, the proposed LDTS generates less overhead and consumes less memory. The dependability-enhanced trust evaluating approach effectively detects and prevents malicious nodes and faulty cluster heads.

Naruephiphat et al. [7] had proposed an innovative clustering algorithm named limiting member node clustering (LmC) algorithm that limits the node members included under each cluster head based on a threshold value. A new cost function is used for selecting the cluster head by taking into account of battery level, energy consumption and its distance to the base station. The transmission range of base stations had been considered for improving the performance of clusters in WSN. The proposed approach provides efficient delivery ratio, increased network lifetime, low latency and less energy consumption when compared with other existing techniques.

2.3 Trust-Based Routing Techniques

Zhou et al. [8] had analysed the WSN based on trust and had proposed a trust behaviour collection technique that behaves like a watchdog. The watchdog transmits the data in multiple hops based on the location of the sensor nodes and the trustworthiness of the target nodes. The proposed technique calculates the trust of nodes and minimizes the cost of energy expended by the watchdog. The proposed technique reduces the life span of the network due to high energy consumption. Also consistent security is not always afforded.

Zhan et al. [9] had designed and implemented a robust trust-aware routing framework for WSNs named trust-aware routing framework (TARF) for securing the multi-hop routing in the dynamic WSN from adversaries. In the proposed technique, each node tracks the trustworthiness of its neighbours and accordingly selects any for transmitting its data. The proposed technique focuses on trustworthiness and energy efficiency. Protection is provided against the replay attacks. TARF is scalable and highly resilient, and the same is proved by comparing it with other existing trust techniques for large-scale WSNs.

Yu et al. [10] had reviewed the trust mechanisms and attacks taking place in the WSNs. The authors had categorized all attacks that take place based on trust in WSN. An intelligent behaviour attack model is implemented to identify inconsistencies in behaviour in the content domain. Various methodologies of trusting techniques had been analysed to provide proper emphasis on trust schemes in WSNs. The proposed approach makes use of Bayesian trust model, entropy trust model, fuzzy trust model, game theory trust model and subjective logic trust model. Behaviour attacks at MAC layer are successfully identified by the proposed approach. Also, efficient protection is not afforded against other security attacks like black hole attack, worm whole attack, selective forwarding and hello flood attack.

Danyang in et al. [11] had studied the critical attacks that could be launched on data transmission in WSNs due to limited energy resource and improper deployment of the sensor nodes. The authors had proposed a trust sensing-based secure routing mechanism (TSSRM) that is lightweight in nature and possessed the ability to thwart several simultaneous attacks. Performance analysis and evaluation of the proposed TSSRM had shown that it affords effective security against a host of attacks. Secure routing algorithms based on trust sensing routing protocols had been proposed for

improving security and overcome common network attacks in the WSN environment. The proposed technique improves the reliability of data transmission in the network when compared to other existing trust-based techniques.

Maarouf et al. [12] had analysed the constrained nature and the prevailing insecurity in WSN and had proposed a trust-aware routing for wireless sensor networks (WSNs) named efficient monitoring procedure in a reputation system (EMPIRE). Reputation-based solutions had been suggested to enforce trust-aware routing where a node needs to continuously monitor its environment for detecting any misbehaviour events that are taking place. Given the resource scarcity present in the WSN, this seems to be a costly affair. The proposed EMPIRE technique is a probabilistic, distributed monitoring methodology that reduces the monitoring activities that are performed by any node and at the same time maintains the attack detecting capability to a satisfactory level. The authors had carried out the simulation using the Monte Carlo simulation technique.

WSNs are generally deployed in security-critical applications, and due to the inherent restrictions in sensor nodes and deployment environment, security can be easily compromised. Present techniques do not efficiently evaluate the trust among nodes and fail to establish energy-efficient routing to enforce security in the WSNs. In order to overcome these issues, energy-efficient clustering and trust-based secure routing scheme are necessary.

3 System Architecture

The proposed approach mainly focuses on energy-efficient clustering and trust-based Sybil attack detection scheme with secure routing in WSNs. The initial process of the secure routing is to form clusters based on location of the nodes and energy. A modified PSO-based clustering algorithm is implemented for cluster formation around the sink coverage area, a process that is initiated by the sink node. The trust and energy of the node calculation as well as Sybil node detection are done by using energy trust system (ETS). ETS consists of two levels of estimation such as CH level estimation and BS level estimation. In CH level estimation, CH receives a control packet from a CM and initiates the verification process. If the CM is legal energy and trust values are estimated based on successful, unsuccessful interaction and timing window, then accepts the packet. Else the CM is illegal that CM is declared as a Sybil node and then deletes the received packet. In BS level estimation, BS receives a packet from a CH and initiates the verification process. If the CH is legal energy and trust values are estimated based on successful, unsuccessful interaction and timing window, then accepts the packet. Else the CH is illegal, that CH is declared as a Sybil node and then deletes the received packet. BS sends the feedback packet via the trusted route to the source CM. Source node transfers the data packet via trusted route to the CH, and CH transfers the data to BS. If the data packet reaches the BS, the BS sends the feedback to its source node. The system architecture had been represented in Fig. 1.

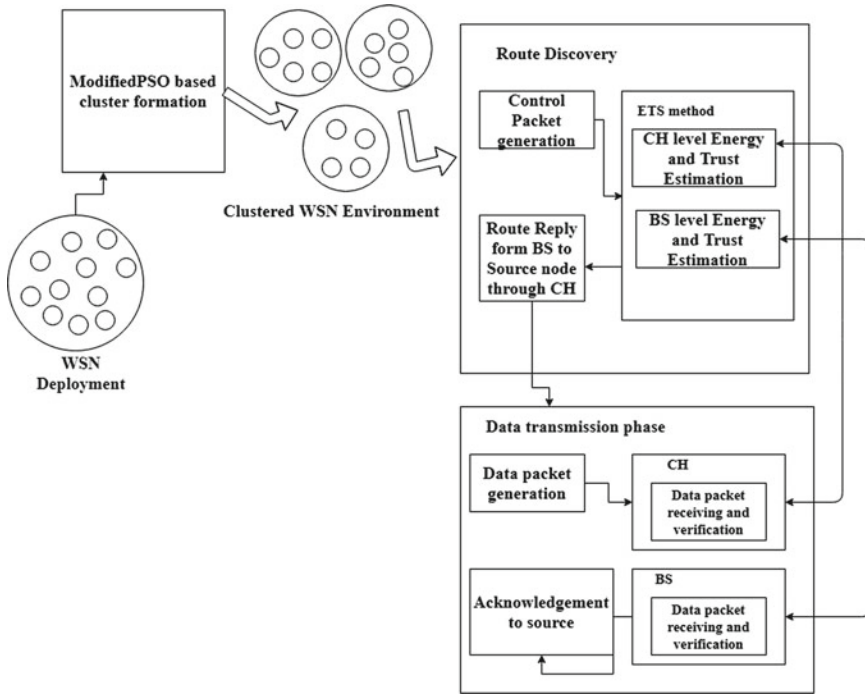


Fig. 1 Energy-efficient clustering and trustable routing

3.1 Cluster Formation

Sensors that are in the vicinity of sink are mostly utilized for delivering data to the sink. Since they are constantly engaged in data transfers, their energy level gets drained up quickly than other nodes. This leads to the formation of hotspots at the sink surrounding area resulting in network isolation. This could be termed as hotspot or energy hole issue. The proposed modified PSO-based clustering algorithm improves the lifetime of the network by reducing the formation of hotspots.

In the modified PSO-based clustering, cluster formation is initiated by the sink node around its coverage area. An info-req-msg is transmitted by the sink to all nodes present in the coverage area. Whenever a message is received by the nodes around sink, they transmit the received message along with the info-reply-msg that contains the sensor-id, position, velocity and current residual energy. The sink node receives the information and updates itself.

Consider a problem space composed of N number of particles in the sink coverage area. The fitness function formulated deduces the particle that has the best value in the swarm and also identifies the best position of each particle periodically. The fitness function for the modified PSO-based clustering is calculated for each particle by equation given below:

$$f_p = a_1x_1 + a_2x_2 + a_3x_3$$

where a_1 and a_2 are weighing parameters that take value between 0 and 1 and $a_3 = 1 - a_1 - a_2$.

$$x_1 = \sum_{i=1}^n \frac{d(\text{current particle member})_i}{c_n}$$

$$x_1 = \sum_{i=1}^n \frac{E(\text{member})_i}{E(\text{current particle})}$$

3.2 Energy Trust System

The proposed work focuses on eliminating Sybil attacks in WSN by developing a lightweight trust-based system that has the capability to carry out multi-level detection mechanism in clustered WSNs. Establishing trust detection system in a clustered topology inside WSN reduces the communication overhead and energy consumed and improves the network scalability and throughput factors. In a heterogeneous WSN with N sensors, there are three entities, namely a base station (BS), cluster heads (CHs) and cluster members (CMs).

In the proposed approach, each sensor node has a unique identity, and positions of every sensor including the BS and CHs are recorded. The sensor nodes are identified by the monitoring node (either BS or CH) based on the information they send that contains their ID, position and energy level along with the sensed data. There are two levels of detection in the proposed ETS, namely cluster head level detection and base station level detection.

3.2.1 Cluster Head Level Detection

Detection is initially carried out at the cluster head (CH) level. Clustering of sensor nodes provides effective topology control. Responsibility of nodes within a cluster is assigned to the respective CH. Whenever a CH receives a message from one of its sensors, it applies the ETS scheme, using verification and trust mechanisms to check the source of that message. It then forwards the data to the BS by performing the following:

1. **Checking**

The cluster head verifies the ID and position of the sender. Once it confirms that the sender of the message is from its own cluster region, it initiates the next

step, namely the trust calculation, else it drops the received message. By doing so, Sybil attacks with forged ID and position can be successfully thwarted.

2. Trust calculation

In this step, the worst-case scenario happening through Sybil attack where the attacker succeeds in impersonating the ID and position of legitimate node is checked. The trust factor $T_{ch,x}$ is deduced as shown in the below equation:

$$T_{ch,x} = - \sum \frac{S_{ch,x}}{S_{ch,x} + U_{ch,x}} - \sum \frac{1}{\sqrt{U_{ch,x}}}$$

where $S_{ch,x}$ indicates the total number of successful interactions between CH with node x , and $U_{ch,x}$ indicates the total number of unsuccessful interactions between CH with node x . If the deduced value is found to be more than 0.3, then the node x is regarded as a trusted node. On the contrary, if the deduced trust value is found to be less than or equal to 0.3, node x is regarded as a Sybil node.

3.2.2 Base Station Level Detection

Second level of detection is carried out at the base station level. In the proposed system, the base station BS is designated as the central command authority. Due to the formation of clusters in the network, the amount of data transmitted to the BS gets reduced. The BS tracks the working of CHs in the network. Whenever a BS receives a message from any CH, it applies the proposed ETS methodology as follows:

1. Checking

Upon receiving a message, the BS verifies the ID and position of the sender. When it ascertains that the sender is an authentic CH, it begins the trust calculation step, else the BS drops the message.

2. Trust Calculation

The trust value $R_{bs,ch}$ is deduced by the BS as follows:

$$R_{bs,ch} = - \sum \frac{S_{bs,ch}}{S_{bs,ch} + U_{bs,ch}} - \sum \frac{1}{\sqrt{U_{bs,ch}}}$$

where $S_{bs,ch}$ indicates the total number of successful interactions between BS with cluster head ch , and $U_{bs,ch}$ indicates the total number of unsuccessful interactions between BS with cluster head ch . If the deduced trust value is found to be more than 0.3, then the cluster head ch is regarded as a trusted cluster node. On the contrary, if the deduced trust value is found to be less than or equal to 0.3, the cluster head ch is regarded as a Sybil node.

3.3 Data Transmission Phase

In the proposed algorithm, both single and multi-path routing are implemented for selecting a near optimal route. A near optimal route with minimum cost, less hop count and maximum residual energy is selected. When an activity happens, the source sensor node transmits data in the shortest path in its corresponding time slice. During its next subsequent time slice, it transmits the next data packet to an alternate neighbour present in its coverage area, regarding it as the best-case multi-path route to traverse towards the sink.

4 Implementation and Results

4.1 Cluster Formation Phase

The sensor nodes are simulated with the help of Network Simulator2. The modified PSO-based clustering algorithm implemented at the sink coverage area by the sink node to form clusters. Once clusters are created, the sink transmits the info-req-msg to the sensors present in its coverage area. Upon receiving the info-req-msg, the sensor nodes send their respective information through the info-reply-msg. This info-reply-msg contains their ID, position, velocity and residual energy. The sink node maintains and updates the received information. The modified PSO-algorithm employed in this work is shown in Algorithm 4.1.

Algorithm 4.1 Modified PSO-based clustering algorithm

- 1: Procedure modified PSO-based clustering ()
- 2: Begin
- 3: Population of N particles are initialized with random positions and velocities
- 4: If target fitness or maximum iteration is not attained
- 5: **for** each particle p in N **do**
- 6: Calculate fitness value (f_p) of each particle
- 7: **if** $f_p > f(pBest)$ **then**
- 8: $pBest = f_p$
- 9: **endif**
- 10: **end for**
- 11: $gBest = \max(pBest \text{ in } P)$
- 12: **for** each particle p in N **do**
- 13: Calculate velocity
- 14: Calculate position
- 15: **end for**
- 16: End while
- 17: End Modified PSO-based clustering

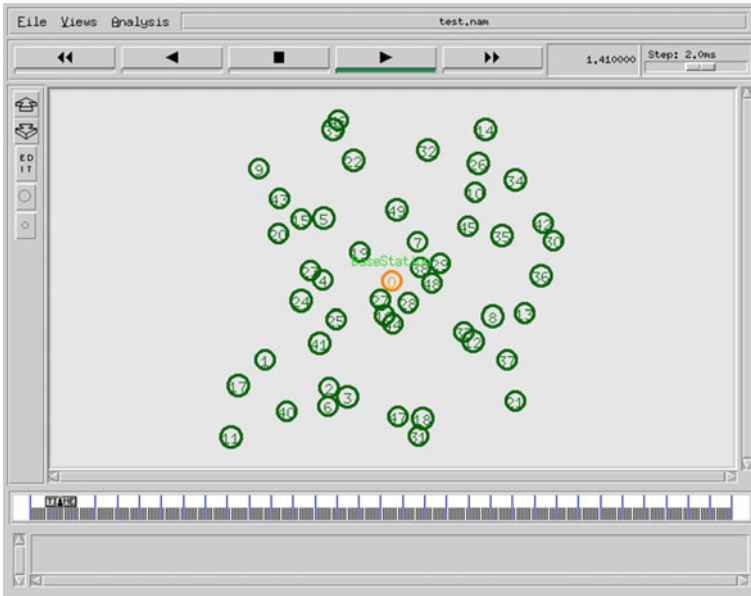


Fig. 2 Network deployment

Figure 2 illustrates the deployment of nodes and network formation. The output of the cluster formation in the network is shown in Fig. 3.

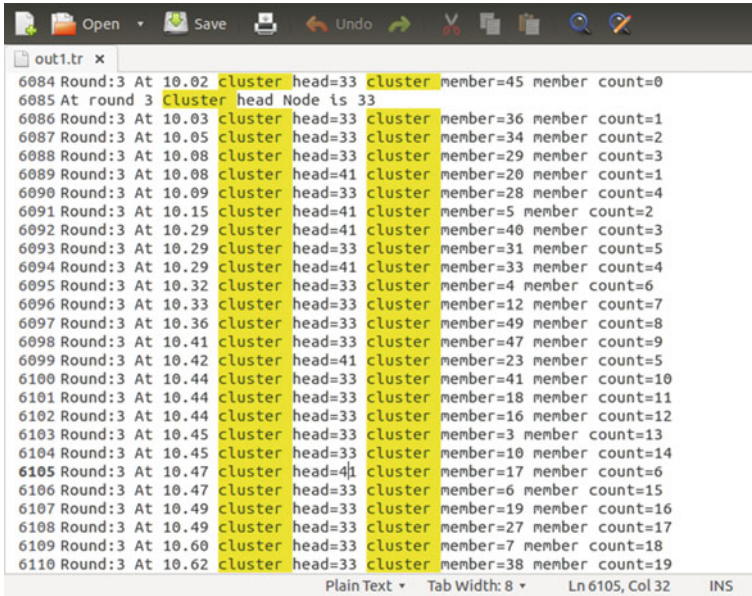
4.2 Energy Trustsystem

Every sensor nodes in the network including the cluster head CHs and base station BS are assigned unique ID and position values. The sensor nodes are identified by the monitoring node which could be either the CH or BS, based on the information they transmit that includes their ID, position, energy level and the actual sensed data. The proposed ETS has two levels of detection, namely cluster head level detection and base station level detection.

Upon receiving a message from any of its members, the cluster CH applies the ETS technique to ascertain the authenticity of the sender using the verification and trust mechanisms. The cluster head level detection algorithm employed in this work is shown in Algorithm 4.2 (Figs. 4 and 5).

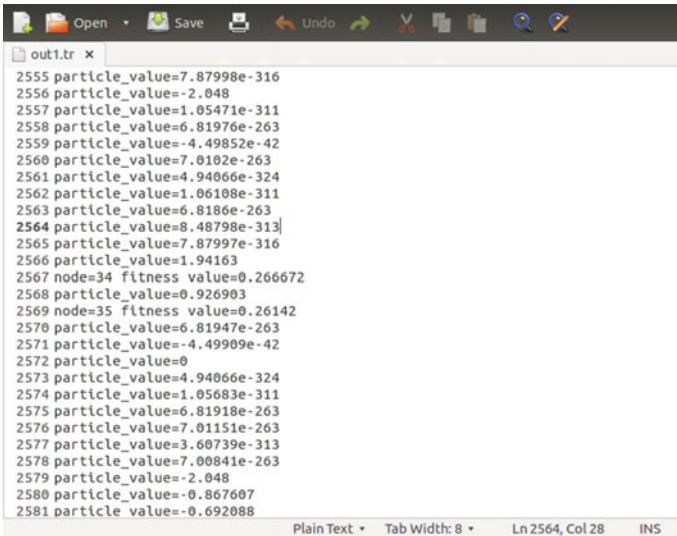
Algorithm 4.2 Cluster head level detection algorithm

- 1: Input: Check whether the message was sent from a legitimate or sybil node.
- 2: Output: Identification of a sybil attack in WSN by applying the ETS.
- 3: Initialize the sensor nodes
- 4: CH receives a message from a CM



```
out1.tr x
6084 Round:3 At 10.02 cluster head=33 cluster member=45 member count=0
6085 At round 3 cluster head Node is 33
6086 Round:3 At 10.03 cluster head=33 cluster member=36 member count=1
6087 Round:3 At 10.05 cluster head=33 cluster member=34 member count=2
6088 Round:3 At 10.08 cluster head=33 cluster member=29 member count=3
6089 Round:3 At 10.08 cluster head=41 cluster member=20 member count=1
6090 Round:3 At 10.09 cluster head=33 cluster member=28 member count=4
6091 Round:3 At 10.15 cluster head=41 cluster member=5 member count=2
6092 Round:3 At 10.29 cluster head=41 cluster member=40 member count=3
6093 Round:3 At 10.29 cluster head=33 cluster member=31 member count=5
6094 Round:3 At 10.29 cluster head=41 cluster member=33 member count=4
6095 Round:3 At 10.32 cluster head=33 cluster member=4 member count=6
6096 Round:3 At 10.33 cluster head=33 cluster member=12 member count=7
6097 Round:3 At 10.36 cluster head=33 cluster member=49 member count=8
6098 Round:3 At 10.41 cluster head=33 cluster member=47 member count=9
6099 Round:3 At 10.42 cluster head=41 cluster member=23 member count=5
6100 Round:3 At 10.44 cluster head=33 cluster member=41 member count=10
6101 Round:3 At 10.44 cluster head=33 cluster member=18 member count=11
6102 Round:3 At 10.44 cluster head=33 cluster member=16 member count=12
6103 Round:3 At 10.45 cluster head=33 cluster member=3 member count=13
6104 Round:3 At 10.45 cluster head=33 cluster member=10 member count=14
6105 Round:3 At 10.47 cluster head=41 cluster member=17 member count=6
6106 Round:3 At 10.47 cluster head=33 cluster member=6 member count=15
6107 Round:3 At 10.49 cluster head=33 cluster member=19 member count=16
6108 Round:3 At 10.49 cluster head=33 cluster member=27 member count=17
6109 Round:3 At 10.60 cluster head=33 cluster member=7 member count=18
6110 Round:3 At 10.62 cluster head=33 cluster member=38 member count=19
Plain Text Tab Width: 8 Ln 6105, Col 32 INS
```

Fig. 3 Cluster formation



```
out1.tr x
2555 particle_value=7.87998e-316
2556 particle_value=-2.048
2557 particle_value=1.05471e-311
2558 particle_value=6.81976e-263
2559 particle_value=-4.49852e-42
2560 particle_value=7.0102e-263
2561 particle_value=4.94066e-324
2562 particle_value=1.06108e-311
2563 particle_value=6.8186e-263
2564 particle_value=8.48798e-313
2565 particle_value=7.87997e-316
2566 particle_value=1.94163
2567 node=34 fitness value=0.266672
2568 particle_value=0.926903
2569 node=35 fitness value=0.26142
2570 particle_value=6.81947e-263
2571 particle_value=-4.49909e-42
2572 particle_value=0
2573 particle_value=4.94066e-324
2574 particle_value=1.05683e-311
2575 particle_value=6.81918e-263
2576 particle_value=7.01151e-263
2577 particle_value=3.60739e-313
2578 particle_value=7.00841e-263
2579 particle_value=-2.048
2580 particle_value=-0.867607
2581 particle_value=-0.692088
Plain Text Tab Width: 8 Ln 2564, Col 28 INS
```

Fig. 4 Fitness value calculation

```

16458 ctime 15.00 start=196
16459 Round:4 At 15.05 cluster head=11 cluster member=6 member count=0
16460 At round 4 Cluster head Node is 11
16461 forward:rtf_up nexthop=11 current_sender=41
16462
16463 Data received by CH 11 from its member 41 MessageID 41 Status 0 Energy
45.850693
16464 It is Not an Attacker Node 41 CH 11
16465
16466 Node 41 is Not a Sybil Attacker Trust of 1.000000 Clustehead 11
16467
16468 CH Level:srid 41 index 11 succ 1 unsucc 0 add 1 root 1.000000 trsut
1.000000
16469 received_count1[index] 1 index 11 memcnt 1
16470 Aggregated Data by CH 11
16471 BS:ch->ach_id 11 cnt11 1 dst 0
16472
16473 @@BS:saddr 11 index 11 daddr 0 ch->ach_id 11 ch->cnid 0 randd 24
16474 forward:rtf_up nexthop=17 current_sender=11
16475
16476 @@BS:saddr 11 index 11 daddr 0 ch->ach_id 11 ch->cnid 0 randd 36
16477 forward:rtf_up nexthop=17 current_sender=11
16478
16479 @@BS:saddr 11 index 11 daddr 0 ch->ach_id 11 ch->cnid 0 randd 23
16480 forward:rtf_up nexthop=17 current_sender=11
16481
16482 BS:GAGAGAGAG 11 saddr 11 ch->ach_id 11 ch->crene 0.000000
    
```

Fig. 5 Cluster head level verification

- 5: CH initializes verification (ID,position,energy) of the CM
- 6: **if** legal ID and position **then**
- 7: Calculate a trust

$$R_{bs,ch} = - \sum \frac{S_{bs,ch}}{S_{bs,ch} + U_{bs,ch}} - \sum \frac{1}{\sqrt{U_{bs,ch}}}$$

- 8: **if** T > 0.3 **then**
- 9: Trusted node and send the message to BS
- 10: **endif**
- 11: **else**
- 12: Delete received message from CM(sybilnode)
- 13: **endif**

In a similar manner, the BS, upon receiving a message from any of the cluster heads CHs, applies the ETS technique to ascertain the authenticity of the sender using the verification and trust mechanisms. The base station level detection algorithm employed in this work is shown in Algorithm 4.3 (Figs. 6, 7 and 8).

Algorithm 4.3 Base station level detection algorithm

- 1: Input: Check whether the message was sent from a legitimate or sybil node.
- 2: Output: Identification of a sybil attack in WSN by applying the ETS.
- 3: Initialize the sensor nodes
- 4: BS receives a message from a CH

```
*out1.tr x
16498
16499 *****BS_VERIFICAION*****
16500
16501 agentBAS:saddr 11 daddr 0 xxx 3.808590 yyy 10.970227 energy 1.500000 adsid
    0 ch->cnid 0 xxx 0.000000 yyyy 0.000000 status 1
16502
16503 ABS: Sybil Attacker is Detected. Node 11 is an Attacker Node BS 0
16504 ABS: Data received by BS 0 from its CH 11 Status 1 Energy 11.748228
16505
16506 ABS:Level:dsid 0 srd 11 succ 0 unsucc 1 add 1
16507
16508 ABS:Node 11 is Sybil Attacker Trust of 0.000000 BS 0
16509
16510 ABS:Level:sid 11 did 11 succ 0 unsucc 1 add 1 root 1.000000 trsut 0.000000
16511 forward:rtf_up nexthop=0 current_sender=16
16512
16513 *****BS_VERIFICAION*****
16514
16515 agentBAS:saddr 11 daddr 0 xxx 3.808590 yyy 10.970227 energy 1.500000 adsid
    0 ch->cnid 0 xxx 0.000000 yyyy 0.000000 status 1
16516
16517 ABS: Sybil Attacker is Detected. Node 11 is an Attacker Node BS 0
16518 ABS: Data received by BS 0 from its CH 11 Status 1 Energy 11.748098
16519
16520 ABS:Level:dsid 0 srd 11 succ 0 unsucc 2 add 2
16521
16522 ABS:Node 11 is Sybil Attacker Trust of 0.000000 BS 0
Plain Text Tab Width: 8 Ln 16522, Col 29 INS
```

Fig. 6 Base station level verification

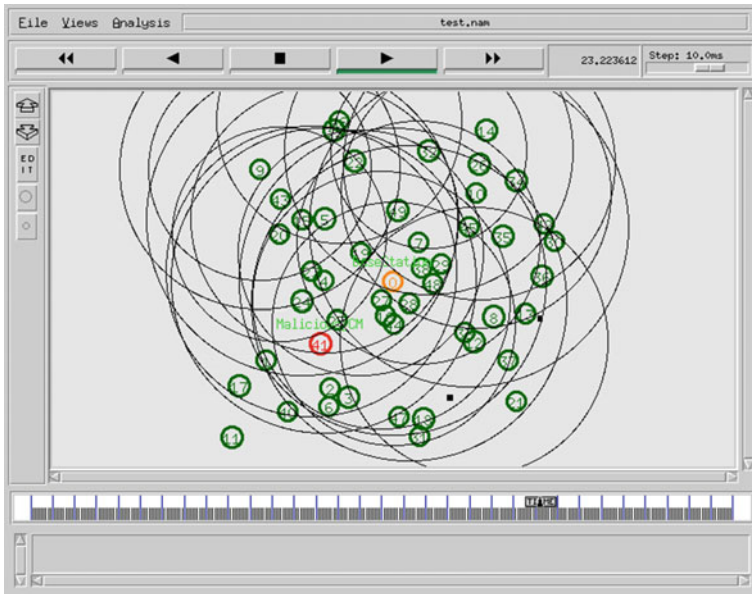


Fig. 7 Sybil attacker node detection

```

*out1.tr x
23793 Round:7 At 30.48 cluster head=11 cluster member=6 member count=3
23794 Round:7 At 30.51 cluster head=10 cluster member=46 member count=1
23795 forward:rtf_up nexthop=22 current_sender=29
23796 forward:rtf_up nexthop=26 current_sender=48
23797 forward:rtf_up nexthop=48 current_sender=49
23798 forward:rtf_up nexthop=45 current_sender=0
23799 forward:rtf_up nexthop=26 current_sender=8
23800 Round:7 At 31.04 cluster head=10 cluster member=35 member count=2
23801 forward:rtf_up nexthop=42 current_sender=45
23802 forward:rtf_up nexthop=41 current_sender=5
23803 Round:7 At 31.27 cluster head=11 cluster member=40 member count=4
23804 Round:7 At 31.37 cluster head=11 cluster member=41 member count=5
23805 forward:rtf_up nexthop=45 current_sender=5
23806 forward:rtf_up nexthop=48 current_sender=20
23807 forward:rtf_up nexthop=45 current_sender=38
23808 forward:rtf_up nexthop=26 current_sender=8
23809 Round:7 At 31.55 cluster head=10 cluster member=29 member count=3
23810 Round:7 At 31.55 cluster head=10 cluster member=7 member count=4
23811 forward:rtf_up nexthop=9 current_sender=46
23812 Round:7 At 31.59 cluster head=10 cluster member=36 member count=5
23813 forward:rtf_up nexthop=28 current_sender=32
23814 forward:rtf_up nexthop=46 current_sender=5
23815 forward:rtf_up nexthop=21 current_sender=37
23816 forward:rtf_up nexthop=46 current_sender=10
23817 Round:7 At 31.80 cluster head=10 cluster member=26 member count=6
23818 Round:7 At 31.84 cluster head=11 cluster member=3 member count=6
23819 Round:7 At 31.87 cluster head=10 cluster member=22 member count=7
Plain Text Tab Width: 8 Ln 17193, Col 29 INS

```

Fig. 8 Data transmission to BS

- 5: BS initializes verification (ID,position,energy) of the CH
- 6: **if** legal ID and position **then**
- 7: Calculate a trust

$$R_{bs,ch} = - \sum \frac{S_{bs,ch}}{S_{bs,ch} + U_{bs,ch}} - \sum \frac{1}{\sqrt{U_{bs,ch}}}$$

- 8: **if** T > 0.3 **then**
- 9: Trusted node and accepts the message
- 10: **endif**
- 11: **else**
- 12: Delete received message from Ch(sybilnode)
- 13: **end**

5 Conclusion

In this paper, data is transferred over multiple nodes in a secured manner. The clustering algorithm is implemented to form cluster nodes. ETS maintains unique ID for each node, and fitness level is calculated using cluster level head detection algorithm. Sybil attacker node is verified before data transmission to BS. Base station level detection reduces attackers. Algorithm like modified PSO cluster algorithm,

cluster level head detection and BS level algorithm are implemented to reduce the attackers' entry during data transmission from node to node.

References

1. Souihli O, Frikha M, Hamouda M (2009) Load-balancing in MANET shortest-path routing protocols. *Ad Hoc Netw* 7:431–442
2. Long J, Dong M, Ota K, Liu A (2014) Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks. *IEEE Trans* 2
3. Lee SJ, Gerla M (2001) Split multipath routing with maximally disjoint paths in ad hoc networks. *Split Multipath*
4. Hu Y, Dong M, Ota K, Liu A, Guo M (2016) *IEEE Syst J* 10:1160–1171
5. Zhang Y, He S, Chen J (2016) Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks. *ACM Trans Netw* 24(3), 1632–1646
6. Li X, Zhou F, Du J (2013) LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. *IEEE Trans Inf Forensics Secur* 8(6)
7. Maarouf I, Baroudi U, Naseer AR (2009) Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks. *IET Commun* 3(5):846–858
8. Zhou P, Jiang S, Aravazhi Irissappane A, Zhang J (2015) Toward energy-efficient trust system through watchdog optimization for WSNs. *IEEE Trans Inf Forensics Secur* 10(3):613–625
9. Zhan G, Shi W, Deng J (2010) TARF: a trust-aware routing framework for wireless sensor networks. In: *European conference on wireless sensor networks wireless sensor networks* pp 65–80
10. Yu Y, Li K, Zhou W (2012) Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *J Netw Comput Appl* 35(3):867–880
11. Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q (2016) Research on trust sensing based secure routing mechanism for wireless sensor network. *IEEE Access*
12. Naruephiphat W, Charnsripinyo C (2010) An energy-aware clustering technique for wireless sensor networks. *Sustain Wirel Sens Netw*