Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A secure routing scheme to mitigate attack in wireless adhoc sensor network

Isaac Sajan R[a,*], *Jasper J*[b]

[a] *Assistant Professor, Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India, 629003*

[b] *Professor, Department of Electrical and Electronic Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India, 629003*

ARTICLE INFO

Article history:
Received 13 November 2019
Revised 16 December 2020
Accepted 10 January 2021
Available online 14 January 2021

Keywords:
False data injection
Carousal attack
Stretch attack
Malicious nodes
Trust mechanism
Secure route

ABSTRACT

Due to the unattended nature and deployment of wireless sensors in the hostile environment, the networks are vulnerable to carousal and stretch attack that causes Denial of Service (DoS). In addition to that, the adversary may also inject bogus data into the network through compromised nodes. This cause the Base Station (BS) to take erroneous decisions and also affects the network's lifetime. To address these issues, the Base Station Controlled Secure Routing Protocol (BSCSRP) is introduced. The proposed work aims to detect the anti-nodes from safe nodes by a trust-based mechanism that secures the network from false data injection as well as provides an efficient route that is free from carousal and stretch attack. The effectiveness of BSCSRP is evaluated by comparing its performance with the existing AF-TNS, BTEM, RSA, and ERF methods.

1. Introduction

Wireless Ad-hoc Sensor Networks (WANET) are employed in many sensitive areas like border security, health care, defense, and so on. These sensors are proficient in making communication with each other without any prior infrastructure. The sensitive data shared by these sensors are prone to attack by attackers. The attackers disable the network with the help of sensitive data. The other kinds of attacks in WANET are vampire attacks, black hole attacks, and jamming attacks (Patel and Soni, 2015; Wazid et al., 2013; Bhushan and Sahoo, 2017). The attacks are targeted on various layers in the network which include the application layer, transport layer, physical layer, and transport layer (Osanaiye et al., 2018). The vampire attack decreases the battery level with its attack behavior. This attack targets to drain the battery resource by sending chunks of malicious data to the sensor nodes. Hence, the detection of a vampire attack is a critical task. A predefined routing encounters the carousal attack, stretch attack, and Fake Data Injection Attack (FDIA) (Vasserman and Hopper, 2013; Nisha et al., 2016; R. Kumari and Sharma, 2017). FDIA is one of the serious problem encountered in wireless sensor networks. This type of attacker modifies or disrupts the data exchange in a network. The FDIA affects state estimation and the security system completely. Some attackers target the switches of substations and equipment's which results in catastrophes (Hu et al., 2018; Lei et al., 2016).

Vampire attacks are categorized on the basis of the stateful protocol and stateless protocol (R. Kumari and Sharma, 2017). In stateful protocol, since the routing path is predefined, the delay in data delivery is minimum. However, the nodes will be

* Corresponding author.
E-mail address: isaacsajanr.001@gmail.com (I.S. R).
https://doi.org/10.1016/j.cose.2021.102197

under the control of the attacker and cannot make independent decisions in case attacked by an adversary. To overcome this issue, stateless protocols can be used in WSN to independently decide the routing path during external or internal attacks. But when it comes to stateless protocol, the network may be affected by the FDIA.

FDIA attacks can inject fake data and cause various types of problems to the Wireless ad-hoc sensor network (Vinodha and Mary Anita, 2018; Kumar and Pais, 2017). Once the adversary compromises a node, the attacker sends false malicious data which may lead to depletion of a large amount of energy, resulting in service denial. In order to secure the network from these attacks, filtering techniques by en-route schemes were implemented (Santhosh and Palanichamy, 2018; Sandhya et al., 2014; Sulochana and Manjula, 2016; Kumar and Pais, 2019; Shahzad et al., 2019; Tariq et al., 2018; Jeba et al., 2013). Also, the carousal and stretch attack degrades the network performance and lifetime by misleading the nodes to select an abnormal route. Hence, it is crucial to introduce an efficient routing scheme to secure the network against these vulnerable attacks.

1.1. *Contributions*

The proposed work aims to detect the anti-nodes from safe nodes as well as secure the routes from carousal and stretch attacks to provide safe routing. This strategy detects the attacked nodes through a trust-based mechanism. The trust-based mechanism checks all the effects of the attack on a node through a child-parent mechanism.

- We include packet drop trust and attribute trust in addition to the existing trust verification measures like direct trust and indirect trust to further improve the security in the network.
- The proposed approach handles the node detection mechanism in the base station part that has an unlimited resource through Base Station Controlled Secure Routing Protocol (BSCSRP). This helps the system to save energy and provide QoS.

The remaining paper is summarized and structured as follows: Section 2 gives the literature review, Section 3 describes the BSCSRP protocol, Section 4 provides the simulation setup and comparative analysis, and Section 5 illustrates the conclusion.

2. Related works

This section provides a review of existing protocols that are intended to secure the network against DoS attacks.

Sreevidya et al., (2018) proposed a security scheme to prevent the injection of false data by employing the Rivest–Shamir–Adleman (RSA) algorithm. It consists of four steps: generation and distribution of key, encryption, en-route filtering, and routing. In the first step, public keys are generated and are distributed to the intermediate nodes. After the generation of keys, the data is encrypted. In the filtering phase, the intermediate nodes verify the data and transmit the packet to the endpoint. This method achieves better performance by dropping the malicious packet.

Padmaja and Marutheswar, (2018) presented a data aggregation algorithm based on trust by eliminating the compromised nodes. This scheme employs a clustering mechanism in which, the nodes that has more residual energy is selected as Cluster Head (CH). If the node is compromised, the trustworthiness of the nodes is verified by the BS. Based on the evaluation, the deviation is found out by the BS. High deviation reduces the value of trust which helps to identify the compromised nodes. This scheme has produced less overhead, energy, and a high network lifetime.

Cui et al., (2017) presented an encryption algorithm by the elliptic curve method to maintain end-to-end confidentiality of data. The proposed method comprises of four phases: (i) Setup (ii) Encryption (iii) Aggregation, and (iv) Verification. In the setup phase, the identity is generated and preloaded into the member nodes and a unique key is shared with all the nodes. In the aggregation phase, a symmetric key is shared with the member nodes and BS. Now, the BS generates a pubic and a private key in which the public key is exposed while the private key is undisclosed. In the encrypted phase, the nodes pick a random number and cipher-text is computed. Finally, the BS verifies the timestamp and decrypts the data.

Kumar and Pais, (2018) presented a combinatorial design-based approach Called En-Route Filtering (ERF) scheme. When an adversary attempts to inject false reports in the network, the intermediate forwarding nodes recognize and delete false reports while forwarding the data to the sink. In this proposed scheme, a secret key is shared with the sensor nodes. After the aggregation of data, the reports are verified by the intermediate nodes. If the report with the secret key is invalid, the packet is immediately dropped. This ensures to drop the false reports before attaining several hops. The combinatorial design secures network communication with low storage overhead.

Yang et al., (2019) presented a distributed filtering scheme to secure the sensor network from the false data injection attack. In this method, each sensor has a protector to choose whether to accept the data based on the information received from the neighboring nodes. When suspicious data is injected by the attacker, the projector determines the vulnerability of the data and the estimator minimizes the state estimation error. This scheme effectively protects the sensor network against hostile attacks.

AlFarraj et al., (2018) proposed an AF-TNS protocol to enhance the security of the network during routing. Here, the trusted path is selected based on direct trust evaluation, energy, and additive metric evaluation. The direct trust is calculated for all the nodes that are in the range of communication-based on the number of packets forwarded and received among the two nodes. In the additive metric evaluation phase, the trusted path is retained by rectification and regression factor identification. From the evaluation, if the trust value drops below the threshold, the malicious node is blocked.

Anwar et al., (2019) Belief Trust Evaluation Mechanism (BTEM) to select a reliable route and protect the network against the DoS attack. The BTEM method comprised of three modules: the traffic monitoring module, the trust evaluation module, and the decision-maker module. The traffic moni-

Table 1 – Comparative Analysis of the Existing Methods.

Author	Technique	Advantages	Disadvantages
Sreevidya et al., 2018	RSA	This method achieves better performance by dropping the malicious packet.	High routing overhead.
Padmaja and Marutheswar, 2018	Trust based data aggregation algorithm	This scheme has produced less overhead, energy, and a high network lifetime.	Energy consumption is more.
Cui et al., 2017	Elliptic curve method	Maintains end to end confidentiality of data and the delay is low.	The computational complexity is high.
Kumar and Pais, 2018	ERF	The combinatorial design secures network communication with low storage overhead.	The packet drop is more.
Yang et al., 2019	Distributed filtering scheme	Secure the sensor network from the FDIA.	Delay is high.
AlFarraj et al., 2018	AF-TNS protocol	High malicious detection rate and network lifetime.	Optimized route is not selected. This decreases the data confidentiality.
Anwar et al., 2019	BTEM	Selects a reliable route and protect the network against the DoS attack.	Network lifetime is less.

toring module is responsible for monitoring the activities of the neighboring nodes by exchanging responses and request packets. The trust evaluation module is responsible for estimating the maliciousness in the network by means of direct trust, indirect trust, and traffic evaluation metrics. Finally, the decision-maker module declares the trustworthiness of the node to decide whether the corresponding node should be blocked or not. Table 1 provides the comparative analysis of the existing methods.

From the above analysis, it is perceived that running complex computations by the nodes consumes additional energy and increases the delivery time. The main task is to provide security to WSN with good Quality of Service (QoS). The authentication mechanism and algorithms to save the nodes from attackers often result in the degradation of the performance. Due to the malicious attacks, the network resource is abused which ultimately depletes the energy. Therefore, an efficient secure routing technique is needed to prevent the network from FDIA, carousal, and stretch attack.

3. Base station controlled secure routing protocol (BSCSRP)

FDIA affects WSN in various ways. It can mimic and alter the sensed data packet that may cause the BS to take a false decision. The effect of carousal and stretch attack also affects the performance of the sensor network. In the stretch attack, the data packets are handled by multiple nodes which in turn causes energy drainage. In the Carousal attack, the data packet is transmitted in a loop form which results in a condition where the same node appears in the route multiple times.

Fig. 1 illustrates the architecture of the sensor network with three clusters. Each node in the network collects the behavioral data of other neighboring nodes and report them with the BS. The BS now lists these data in a table and evaluates the behavioral data by a trust mechanism. From the evaluation report, the nodes in the network with low trust values are blocked and a new routing path is selected.

3.1. *Assumptions*

- The attacker can overhear the data during transmission and introduce false data into the network.
- Every sensor node in the network has a limited energy resource whereas, the sink has unlimited energy.
- The adversary cannot compromise the sink node.
- Each node in the network has similar processing power, attributes, and routing algorithm.
- Malicious nodes cannot interact with each other.

3.2. *Threat model*

For a compromised node, all the data that is stored in the nodes are exposed to the attacker. Based on the obtained information, the attacker may inject false data by altering the genuine packets. This may lead to taking incorrect decisions by the BS. Moreover, if the compromised nodes are not detected, more false data may get injected into the sink resulting in DoS.

Fig. 2(a) shows the effect of the carousal attack in which the data packets are transmitted again and again on the same route. Fig. 2(b) depicts the effect of the stretch attack in which the packets are forwarded through a long route before reaching the destination. Fig. 2(c) illustrates FDIA where the original data packet is altered by the attacker. According to the BSCSRP protocol, the base station allocates the path which is not attacked by the FDIA as well as Carousal and Stretch attack after acknowledging the request from the source.

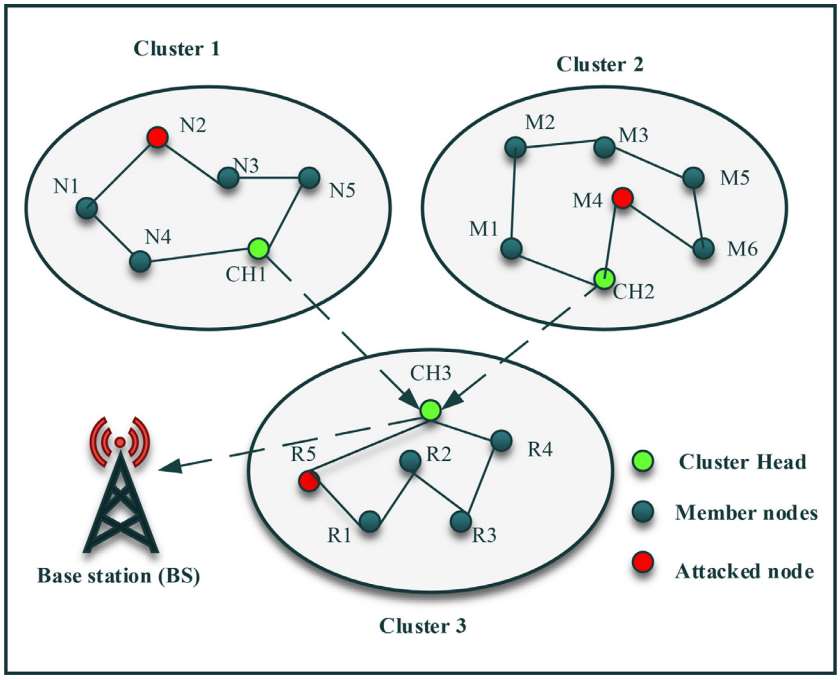
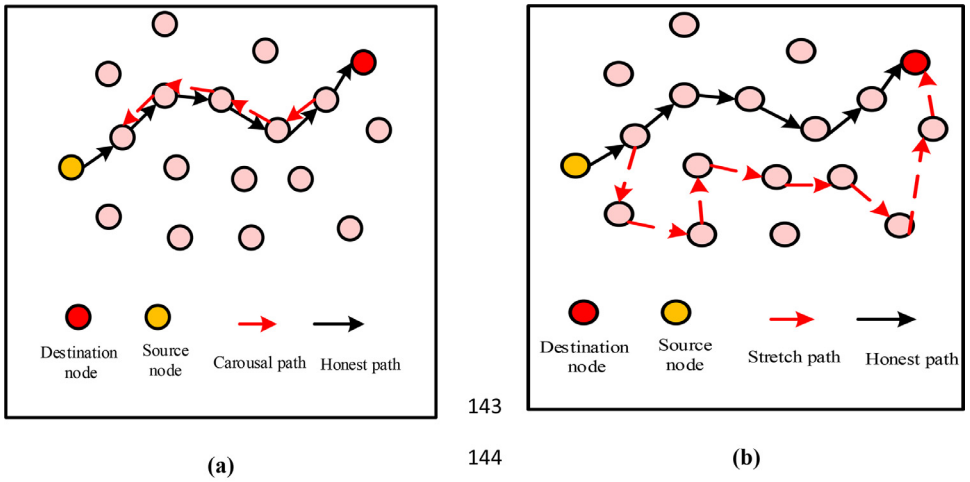
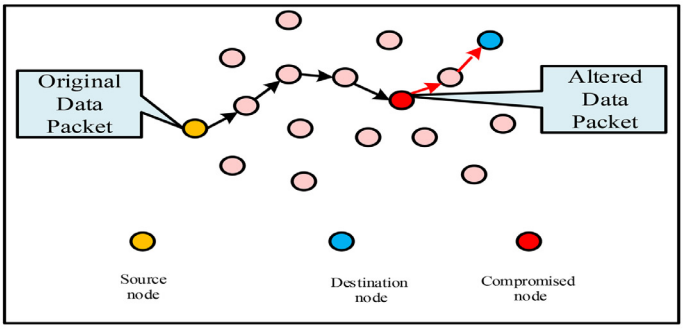


Fig. 1 – Architecture of the sensor network.



(a) (b)



(c)

Fig. 2 – (a) Carousal attack (b) Stretch attack (c) Fake data injection attack.

3.3. Cluster formation

The sensors are deployed in the network with the formation of clusters. Each cluster has a CH and member nodes in which, the CH is accountable for aggregating the data from the member nodes and share it with the BS. The CH is nominated such that the distance to BS as well as to the neighboring sensor nodes are minimum. This approach helps to transfer the data packet quickly with reduced time delay.

3.3.1. Distance measurement

The distance between two nodes N and M with location(N_x, N_y) and (M_x, M_y) is determined by,

$$d(N,M) = \sqrt{(M_x - N_x)^2 + (M_y - N_y)^2} \tag{1}$$

Based on the Euclidean measurement, the node that is closest to the center of the cluster attains the highest chance of becoming CH.

3.3.2. Energy consumption

The energy of the sensor is utilized during sensing, data aggregation, transmission, and reception.

The energy loss during transmission is given by,

$$E_{tx} = \begin{cases} E_{el} * g + g * \varepsilon_{fs} * d^2 & d < d_0 \\ E_{el} * g + g * \varepsilon_{mp} * d^4 & d \geq d_0 \end{cases} \tag{2}$$

where $d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$, d represents the separation distance,E_{el} is the energy required to operate the receiver or transmitter circuit, and g implies the number of bits.

The energy required to receive 'g' bits of packets is given as,

$$E_{rx} = E_{el} * g \tag{3}$$

The total energy spent is given as,

$$E_{con} = E_{tx} + E_{rx} \tag{4}$$

The residual energy of the sensor node,

$$E_{res} = E_{\text{int}} - E_{con} \tag{5}$$

where $E_{\text{int}}$is the node's initial energy.

3.3.3. Threshold

The CH is selected in each round depending on the threshold energy of the nodes. This mitigates the problem of selecting the nodes with less residual energy than CH.

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r \bmod \frac{1}{P}\right)} \times \frac{E_{res}}{E_{\text{int}}} & if\ n \in S \\ 0 & Otherwise \end{cases} \tag{6}$$

Here, P is the probability of a sensor node to become CH, r indicates the round, and S represents the number of nodes other than CH. The CH selection process is provided in Algorithm 1.

Algorithm 1 – Energy-aware CH selection

Input: Get the location of the nodes
Output: Elect the most efficient node as CH
for i = 1,2,3,..n
do Calculate the distance between the nodes
Calculate the transmission energy,

$$E_{tx} = \begin{cases} E_{el} * g + g * \varepsilon_{fs} * d^2 & d < d_0 \\ E_{el} * g + g * \varepsilon_{mp} * d^4 & d \geq d_0 \end{cases}$$

Calculate the energy consumed during reception,

$$E_{rx} = E_{el} * g$$

Determine the residual energy of the nodes,

$$E_{res} = E_{\text{int}} - E_{con}$$

Determine the threshold value for each nodes
for min d(M,N) and T(n)<0.05 **do**
Elect as CH
Else
join as member node
end for

3.4. Trust verification model

BSCSRP formulates a trust model to choose the safe route. Since the adversary cannot get detailed knowledge about the real-time sensor parameters and network information, the attacker can only inject the data in the network with his own understanding. The base station broadcasts a behavior ID to each of the nodes from a table which is maintained in the BS. The table is designed based on the behavior of the network and real-time parameters of a sensor like energy, time to deliver a packet, repetition of packet processing by a node, increase of packet route length, etc. The trust evaluation efficiently analyzes the anomaly behavior. Every child node analyzes the behavior of the parents and inform the base station regarding the behavior of the nodes. The BS in turn compares the information with the original information and reports the unsafe behavior ID to other genuine nodes in the network.

3.4.1. Direct trust (DT)

The direct trust is found out based on the interaction among two nodes as given in Eqn. (7).

$$DT = \frac{P_{rec}(i)}{P_{for}(j)} \tag{7}$$

where, $P_{rec}(i)$ denotes the successfully received packets by node I and $P_{for}(j)$ denotes the quantity of packets forwarded by node j.

3.4.2. Indirect trust (IT)

Indirect trust is determined based on the data collected from the nearby nodes. Consider node 'i' wants to find out the trust of node j to forward a packet but, it has no previous communication history with node j. In this case, node i gets the trust degree of node j from its neighboring nodes.

$$IT = \frac{1}{k} \sum_{m=1}^{k} DT(m) \tag{8}$$

where k denotes the total number of neighbors of node j, DT is the direct trust calculated from Eqn. (7).

3.4.3. *Packet drop trust (PDT)*

Drop trust is the trust that is calculated based on the previous packet drop history with its neighbors.

$$PDT = \frac{1}{k}\sum_{m=1}^{k}\frac{PD_k}{PS_{i,k}} \tag{9}$$

$PS_{i,k}$ denotes the total number of packets previously sent by node i to neighboring node k, PD_k denotes the number of packets dropped by the neighboring node k that was previously received from node i. In this way, if the packet drop trust of a node is close to 1, then it represents that the node is untrustworthy.

3.4.4. *Attribute trust (AT)*

Before the deployment of the sensors, each node is assigned with some attributes such as language, country, source ID, destination ID, location of the destination node, key, and Type of service that are similar to each other. During communication, each node checks whether the neighboring next-hop node has a common interest with each other by using the Eqn. (10).

$$\mathrm{AT} = \frac{N_{com}(t)}{N_{att}(t)} \tag{10}$$

where, $N_{att}(t)$ is the total number of attributes, and $N_{com}(t)$ denotes the number of common attributes. Based on this calculation, if the number of common attributes is less, then it emphasizes that the trust degree is low. If the attribute ratio is unity, then it denotes that the node has a higher trust degree.

$$\text{Total Trust} = \alpha\mathrm{DT} + \beta\mathrm{IT} + \gamma\mathrm{PDT} + \delta\mathrm{AT} \tag{11}$$

$\alpha, \beta, \gamma, \delta \in [0, 1]$ are the weight values such that $\alpha + \beta + \gamma + \gamma = 1$

By evaluating Eqn. (11), 0 denotes low trust and 1 denotes high trust.

3.5. *Energy efficient secure route selection*

This section provides the evaluation of the parameters that are to be considered in selecting a path that is secure as well as energy-efficient. The secure path selection process consists of identifying the safe path for data transmission. This indicates the path is not affected by false data injection, Carousal, and Stretch attack. During data transmission, the nodes check the presence of antinodes with the information obtained from trust evaluation in Section 3.4. The nodes disconnect their connection with the compromised nodes and select a route that does not have any compromised nodes. Furthermore, in order to select an energy-efficient route, the energy, distance, and delay in communication are also estimated as follows.

3.5.1. *Energy resource*

To have balanced energy depletion in the sensor field and to enhance the lifetime, the intermediate sensor nodes with maximum residual energy has to be selected.

$$\mathrm{ER} = \begin{cases} E_{res} < E_{th} & 0 \\ E_{res} > E_{th} & 1 \end{cases} \tag{12}$$

E_{res} is the residual energy of the sensor that is calculated from Eqn. (5), and E_{th} denotes the threshold energy. Here $E_{res} < E_{th}$ indicates that the node is untrustworthy and returns 1, $E_{res} > E_{th}$ signifies that the node can be trusted hence, return 1.

3.5.2. *Distance*

When the network is subjected to vampire attacks like carousal and stretch attacks, the delay in delivering the data packets increases due to the abnormal selection of the longer route. The distance between the neighboring node and the destination with location (x_1, y_1) and (x_2, y_2) is determined by,

$$d(N, D) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{13}$$

The neighboring node that is in the minimum distance to the destination is chosen for the next-hop to transmit the packet. This helps to deliver the packet with less delay and also enhances the network lifetime.

3.5.3. *Latency*

It is also important to send the packet to the neighboring node that responds quickly than other nodes to ensure quick data delivery.

3.5.3.1. *Propagation delay (PD)* It is the duration for the packet to reach the receiver and is determined as given in Eqn. (14).

$$PD = \frac{d(s, d)}{v} \tag{14}$$

$d(s, d)$ is the distance between the source node to neighboring nodes, v denotes the speed of transmission medium.

3.5.3.2. *Serialization delay (SD)* It is the time taken to encode the bits of the data packet. The delay increases as the length of the packet increases.

$$SD = \frac{PS}{Txr} \tag{15}$$

PS denotes the packet size, Txr denotes the data transmission rate.

$$Lt = PD + SD \tag{16}$$

Overall the transmission route is selected such that the nodes in the chosen path have max (Trust), max (ER), min d(N,D), and min (Lt). Fig. 5 gives the flowchart for the BSCSRP method.

3.6. *Malicious node isolation*

Once the base station forwards the behavior ID of the attacked node to all of the sensors in the network, safe nodes disconnect the connection with the antinode and completely isolates them. Fig. 3 demonstrates the flowchart for the proposed BSCSRP protocol. Energy efficient safe route selection process is provided in Algorithm 2.

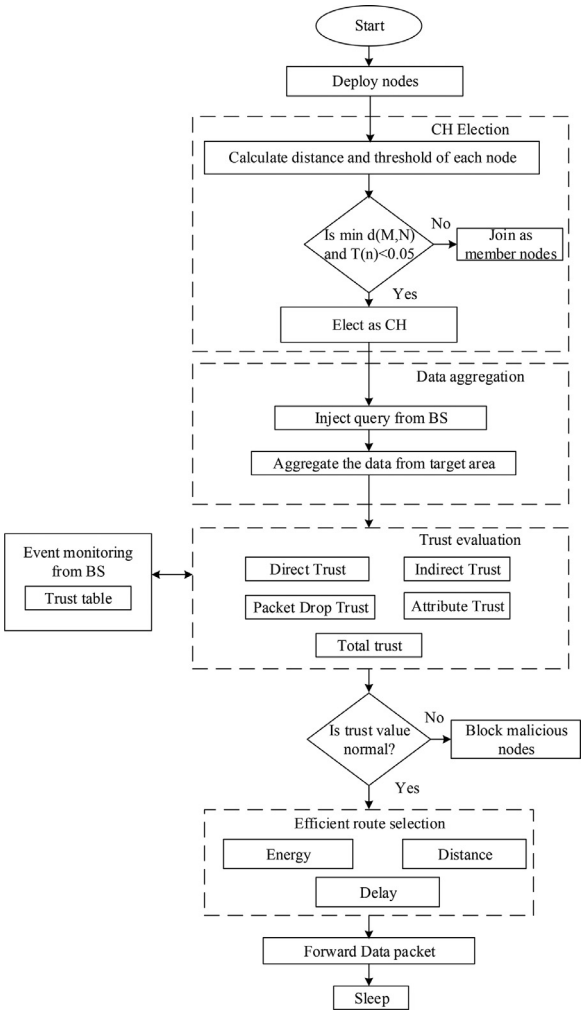


Fig. 3 – Flowchart for the proposed BSCSRP protocol.

Algorithm 2 – Energy efficient safe route selection

Input: Data from each next hop neighboring nodes
Output: Genuine next hop neighbor
for each next hop neighboring node **do**
compare the residual energy of the senor nodes with the threshold value

$$ER = \begin{cases} E_{res} < E_{th} & 0 \\ E_{res} > E_{th} & 1 \end{cases}$$

calculate the distance between the neighboring node and the destination

$$d(N,D) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

calculate the delay/latency in communication with the neighboring nodes

$$Lt = PD + SD$$

for the node with max (Trust), max (ER), min d(N,D), and min (Lt) **do**
select as next hop forwarding node
else
choose alternate path and report the node with low trust
end for
end for

Table 2 – Parameters of the network.

Parameters	Value
Area of the network	100 m^2
Number of sensors in the network	100
Position of the base station	(100,10)
Initial energy of sensor node	1.0 J
Communication range of member nodes	30m
Communication range of CH	50 m
Transmission energy	0.01 J
Receiving energy	0.01 J
E_{elec}	50 nJ/bit
ε_{mp}	0.0013 pJ/bit/m^2
ε_{fs}	10 pJ/bit/m^2
Transmission medium speed (km/s)	300,000
Data packet size (bytes)	500
Data transmission rate (Mbps)	1
Threshold value of CH	0.05
Number of malicious nodes	10–50

4. Experimental result and simulation setup

The simulation is tested in MATLAB and the performance of BSCSRP is evaluated under false data injection, Carousal and Stretch attacks in terms of energy consumption, delay, Packet Delivery Ratio (PDR), detection rate, detection accuracy, and throughput.

4.1. *Simulation setup*

The performance of BSCSRP is tested in MATLAB by deploying 100 nodes in a simulation area of$100m \times 100m$. The remaining parameters are listed in Table 2.

4.2. *Routing model*

Fig. 4 shows the division of the network with several clusters with each cluster having a CH. Under the honest scenario, the source node 0 aggregates the data and forwards it to the BS in a genuine path (0–56–8–80–38–64–68).

Fig. 5(a) shows the routing path of the data packet without the presence of the BSCSRP protocol. In this, the adversary compromises nodes 14, 36,43,53,55, and 87 in order to drain the energy by employing the carousal attack. Due to the carousal attack, instead of choosing the genuine path (0–56–8–80–38–64–68), the nodes choose the path in closed-loop (0–56–8–80–38–53–55–48–87–83–10–8–80–38–64–68). Fig. 5(b) illustrates the honest path taken by the influence of BSCSRP protocol represented in the black arrow.

Fig. 6(a) gives the representation of the network affected by the stretch attack without a secure routing protocol. Due to the presence of compromised nodes in the network, the data packet is transmitted in a longer route (0–56–8–14–36–21–10–83–87–89–48–55–38–64–68) than the usual path. Fig. 6(b) shows the honest path (0–56–8–80–38–64–68) taken by BSCSRP protocol.

Fig. 7(a) sketches the effect of false data injection without the effect of the BSCSRP protocol. In this, the adversary compromises node 55 and injects suspicious data into the

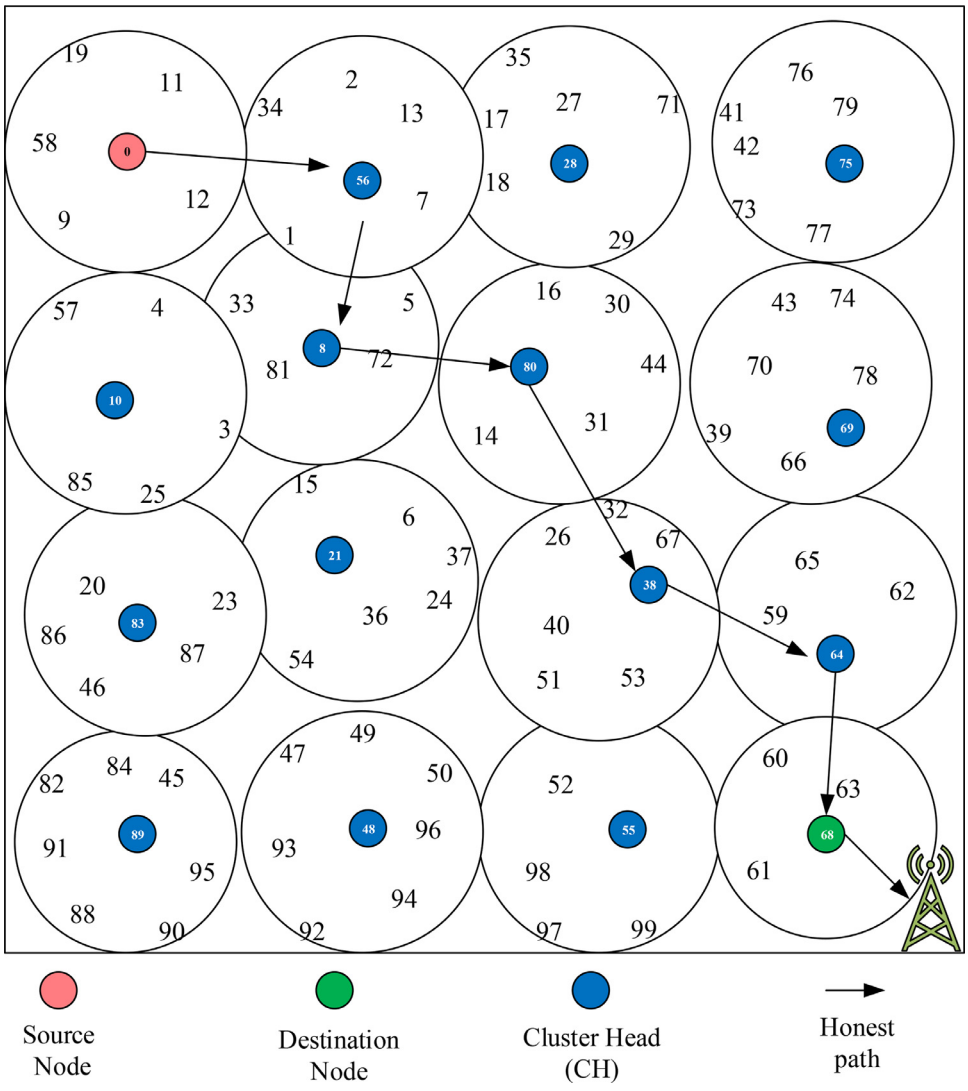


Fig. 4 – Honest scenario.

field. This may lead to take false decision by the BS. Whereas, Fig. 7(b) sketches the path taken by the BSCSRP protocol. Here, node 55 is blocked due to its maliciousness which is found out by the trust mechanism given in Section 3.4. After the blockage of the compromised node, a new CH is elected for that particular cluster and a dynamic route is established.

4.3. *Comparative analysis*

The proposed BSCRP protocol is compared with the existing, RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019) protocol for the metrics such as energy consumption, throughput, end to end delay, detection rate, detection accuracy, and False Positive Rate (FPR).

4.3.1. *Energy consumption*

The amount of energy consumed by the nodes determines the network's lifetime. More energy consumption decreases the network's lifetime. Fig. 8 shows that the residual energy of the nodes by comparing them with the existing RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019) methods. The proposed BSCSRP scheme consumes less energy since it mitigates against carousal and stretch attacks that cause the data packet to take a longer route. The elimination of these attacks provides the most secure and shortest. Therefore, due to the minimal energy consumption by the BSCSRP approach, the residual energy is more than 65% even in the presence of 50% malicious nodes.

4.3.2. *Average throughput analysis*

Fig. 9 illustrates the acquired average throughput for the BSCSRP under a varying number of malicious nodes. It can be seen that the throughput for all the methods decreases as the number of antinodes increases. However, the proposed BSCSRP protocol has the highest average throughput compared with the existing RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019) schemes.

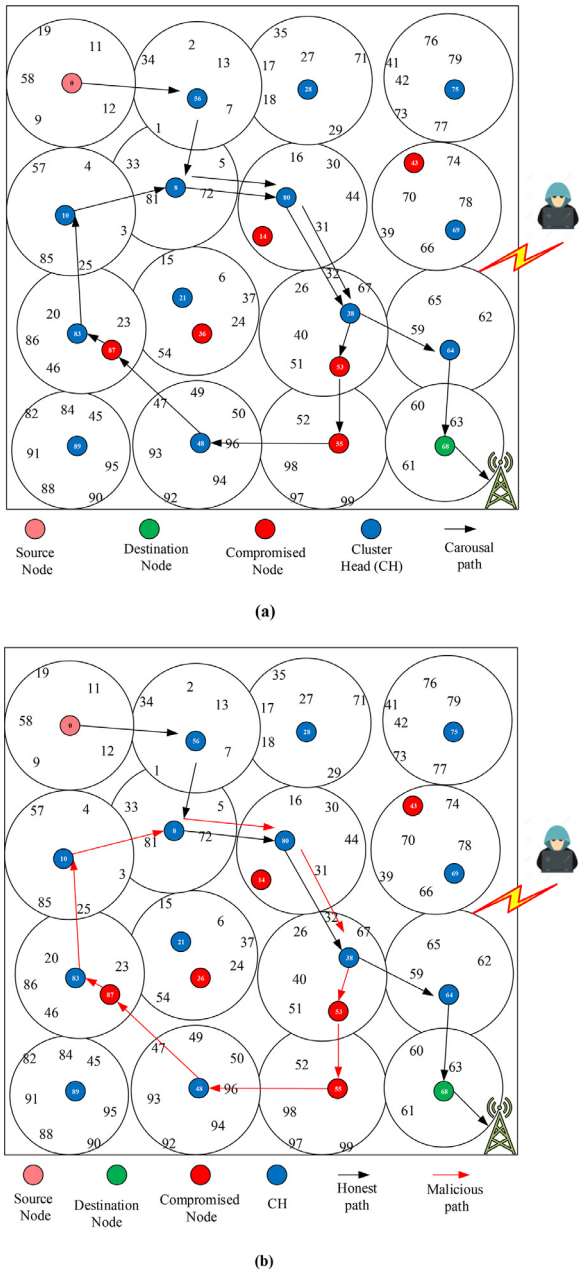


Fig. 5 – Carousal attack (a) without BSCSRP protocol (b) with BSCSRP protocol.

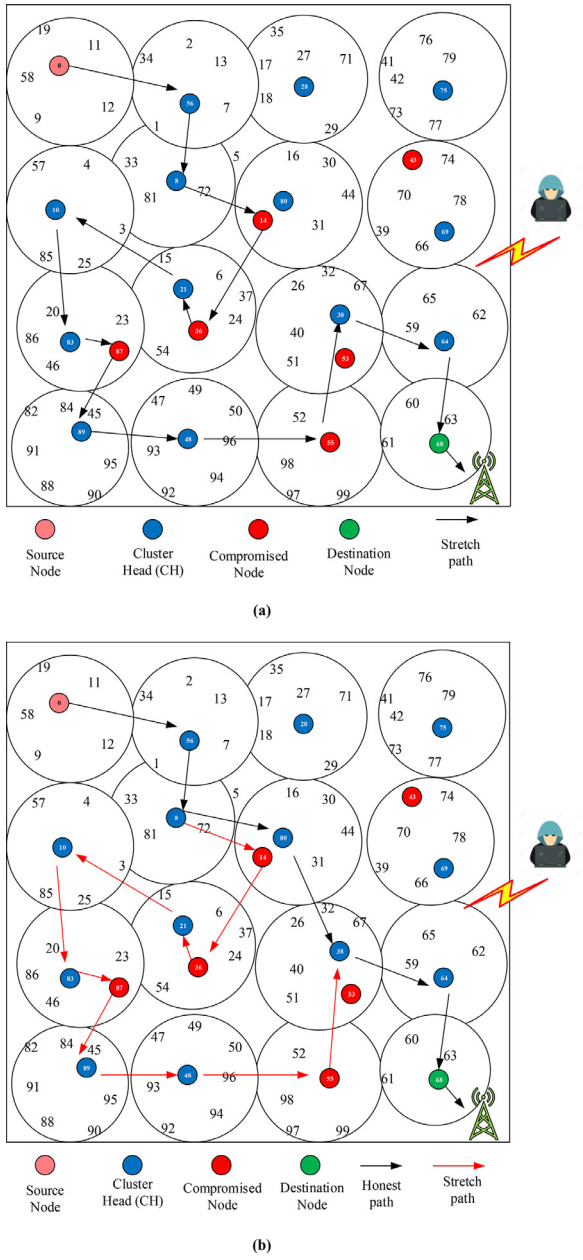


Fig. 6 – Stretch attack (a) without BSCSRP protocol (b) with BSCSRP protocol.

4.3.3. *End to end delay*

End to end delay is the time interval for the data packet to reach the destination. The delay in delivering the packet for BCSRP, BTEM, AF-TNS, ERF, and RSA under 50% compromised nodes are 0.024 s, 0.035 s, 0.041 s, 0.049 s, and 0.055 s respectively. The proposed protocol selects a route with minimum distance to the destination and the packet is only forwarded to the neighboring nodes that respond quickly than other nodes. Therefore, when making a comparison in Fig. 10, the delay in data delivery is minimum for the proposed BSCSRP approach than AF-TNS and BTEM.

4.3.4. *Detection rate*

Fig. 11 shows the detection rate of antinodes in the sensor field in percentage. The detection rate is analyzed by deploying 10–50 malicious nodes in each experiment. The analysis proves that the BSCSRP approach has the highest detection rate at each round. From the observation, the detection rate is almost 100% for the proposed BSCSRP scheme including the existing RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019) in the presence of 10% malicious nodes. But, as the number of compromised nodes increases, the detection rate of the AF-TNS and BTEM is less than that of the proposed method.

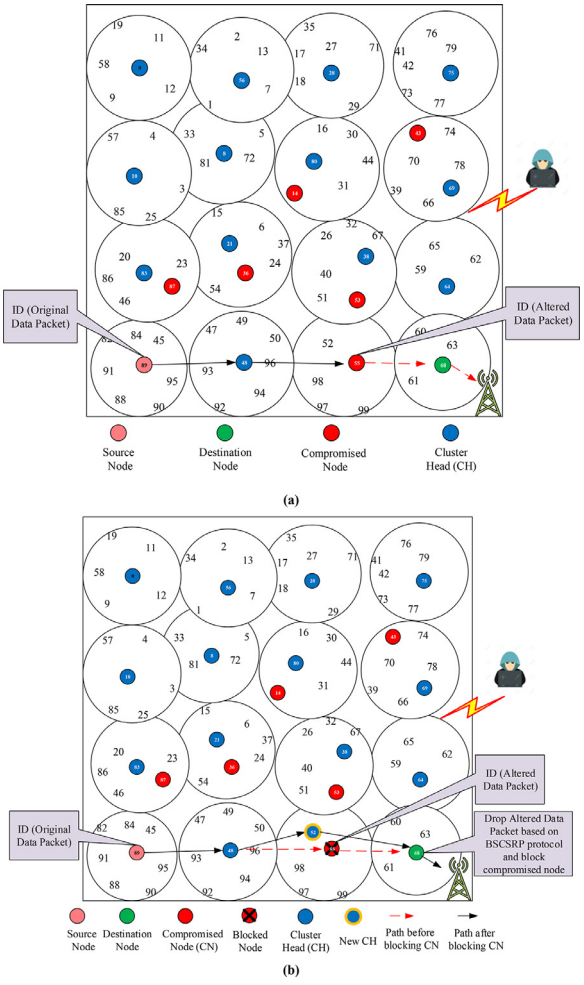


Fig. 7 – Fake data injection (a) without BSCSRP protocol (b) with BSCSRP protocol.

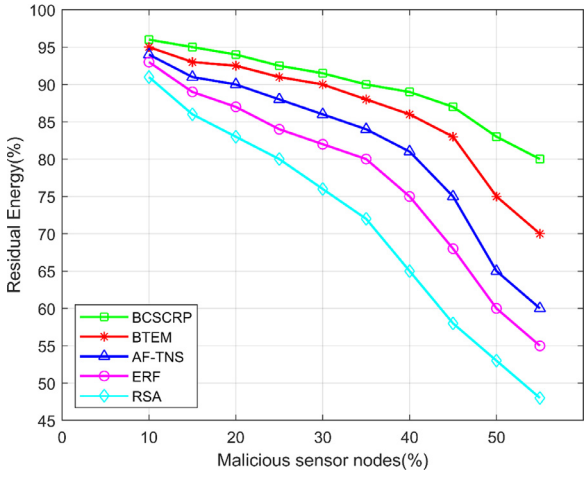


Fig. 8 – Energy Consumption Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

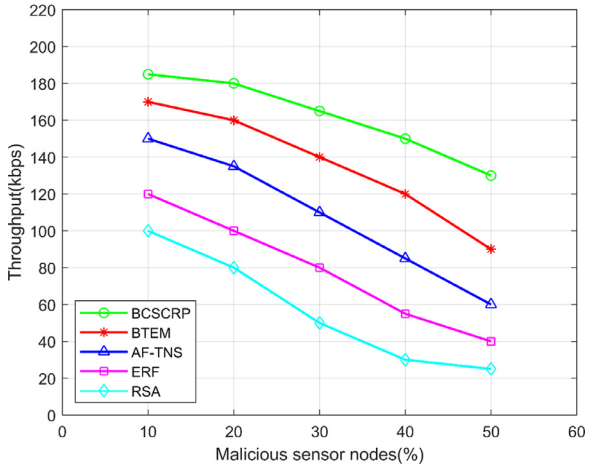


Fig. 9 – Average throughput analysis by varying the number of malicious nodes from 10% to 50%.

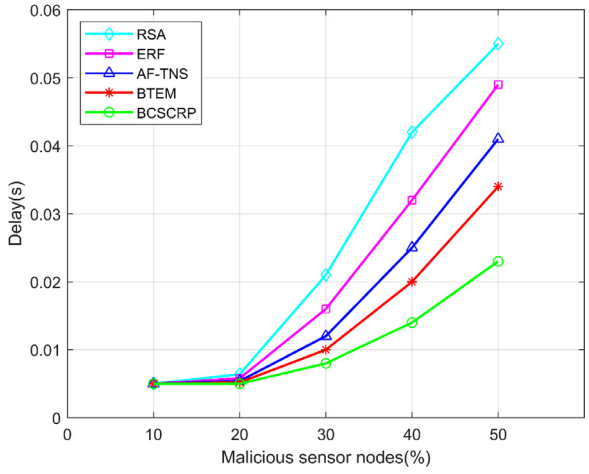


Fig. 10 – End to End Delay Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

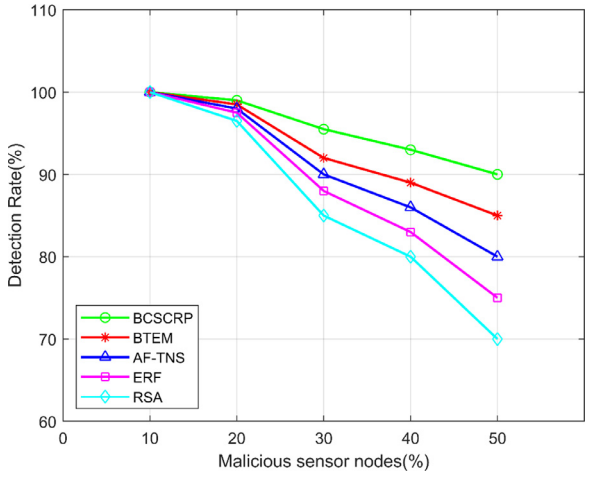


Fig. 11 – Detection Rate Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

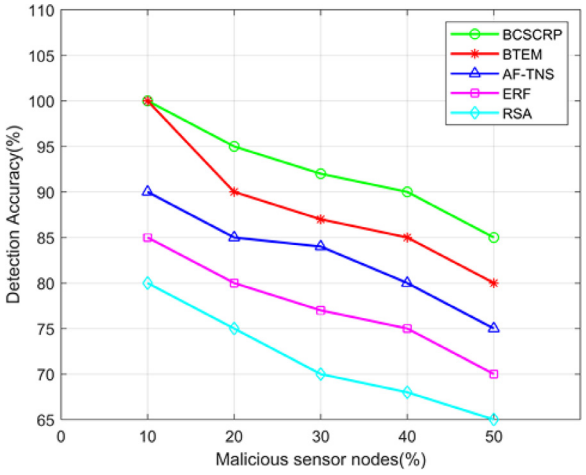


Fig. 12 – Detection Accuracy Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

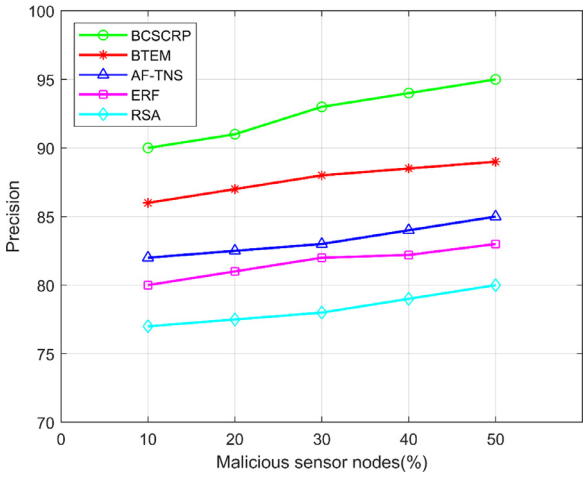


Fig. 14 – Precision Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

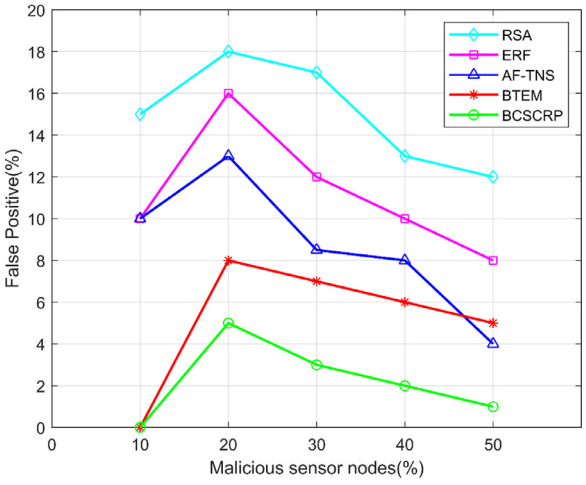


Fig. 13 – False Positive Rate Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

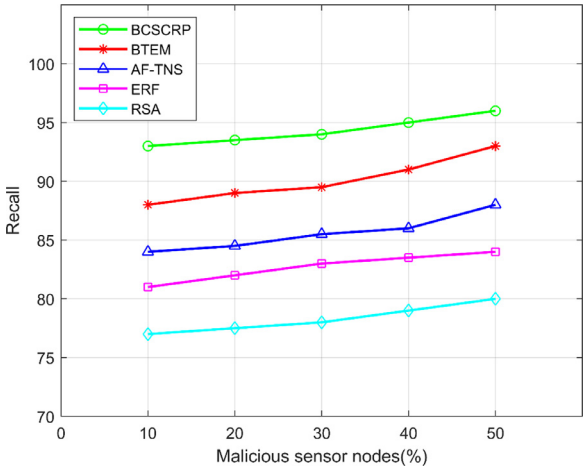


Fig. 15 – Recall Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

4.3.5. *Detection accuracy*

Fig. 12 shows the accuracy of the BSCSRP protocol. The accuracy of the BSCSRP in the presence of 50% malicious nodes is 85%. Whereas, the existing BTEM and AF-TNS have lower accuracy. The increase in accuracy for the proposed method is because the existing schemes only consider direct trust and indirect trust for determining the secure route. Whereas, the proposed BSCSRP method evaluates the Packet Drop Trust (PDT) and Attribute Trust (AT) in addition to the direct and indirect trust. The addition of PDT and AT improves the security as well as the detection accuracy.

4.3.6. *False positive rate*

Fig. 13 shows the analysis conducted for False Positive Rate (FPR) for the methods AF-TNS, BETM, and BSCSRP. The number of antinodes that are wrongly classified as genuine nodes is False Positives (FP) and the nodes other than malicious nodes are classified under True Negative (TN). The FPR is analyzed by deploying 10–50 malicious nodes at an experiment in which, the FPR is determined using, $FPR=FP/FP+TN$. Based on this understanding, the FPR for the BSCSRP and BTEM is 0 under 10% malicious nodes. Whereas, the FPR for the existing AF-TNS method is higher than the BSCSRP approach of about 10%. This improvement in BSCSRP is due to the introduction of the efficient trust mechanism that considers the similarity in attributes, the previous history of packets dropped by the nodes, the quantity of the packet delivered successfully, DT, and IT.

Fig. 14 provides the precision analysis with the existing methods. From the analysis, it observed that the precision of the proposed BSCSRP is higher than other existing schemes. The precision of the existing RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019) are 80%, 83%, 85%, and 89%. Whereas, the precision of the proposed BSCSRP approach is 95%.

Fig. 15 provides the recall analysis with the existing methods. From the analysis, it observed that the recall of the proposed BSCSRP is higher than other existing schemes. The re-

Table 3 – Metrics compared with existing techniques under 50% malicious nodes.

Method	Residual Energy (%)	Average Throughp-ut (kbps)	Delay (*sec*)	Detection rate (%)	Detection accuracy (%)	FPR (%)	Precis-ion	Rec-all	F1-score
AF-TNS	65	60	0.041	80	75	4	85	88	87
BTEM	75	90	0.035	85	80	5	89	93	93
RSA	54	25	0.055	70	50	12	80	80	80
ERF	60	40	0.049	75	70	8	83	84	84
BSCSRP	84	130	0.024	90	85	1	95	96	94

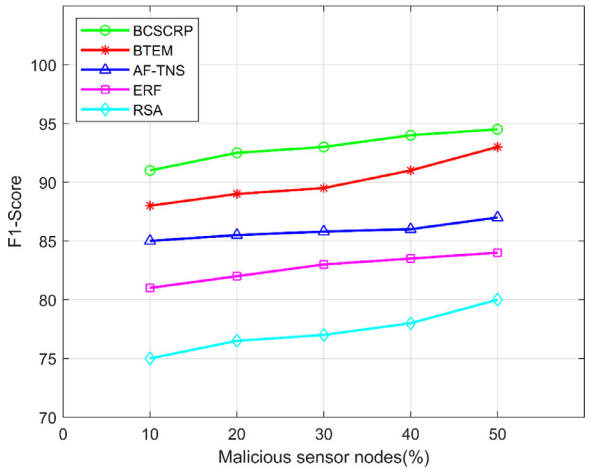


Fig. 16 – F1-score Analysis by Varying the Number of Malicious Nodes from 10% to 50%.

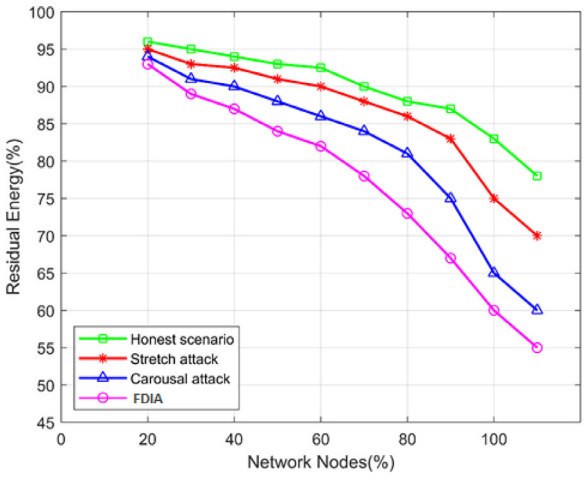


Fig. 17 – Energy consumption of BSCSRP protocol under various attacks from 10% to 50%.

call score of the proposed BSCSRP is higher than the existing RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019).

Fig. 16 provides the F1-score obtained for the proposed BSCSRP and the existing methods. From the analysis, it observed that the F1-score of the proposed BSCSRP is higher than other existing scheme.

Fig. 17 gives the energy consumption analysis for the proposed BSCSRP protocol under various attacks. Under honest scenario, it is observed that the energy consumption is low whereas, under the presence of carousal, stretch, and FDIA attack, the network consumes more energy than the honest scenario. Table 3 gives the performance comparison of the BSCSRP approach with the existing RSA (Sreevidya et al., 2018), ERF (Kumar and Pais, 2018), AF-TNS (AlFarraj et al., 2018), and BTEM (Anwar et al., 2019) schemes by deploying 50% malicious nodes in the network.

5. Conclusion

Deploying wireless sensors in information sensitive areas like the military with secure protection schemes is of prime importance. In WSN, the integrity of the data can be distorted by the compromised nodes by injecting false data or by vampire attacks like carousal attack and stretch attack. These attacks deplete more energy in the WANET and cause DoS. Moreover, the lifetime and performance of the WANET also get degraded because of the abnormal route selection. Hence, we propose BSCSRP to enhance the security of the network in the presence of carousal, stretch, and false data injection attacks. The BSCSRP scheme works based on direct trust, indirect trust, attribute trust, and packet drop trust. This trust evaluation benefits the network by protecting the network against DoS attacks. The security-based trust mechanism provides a simple and stronger solution to the network by analyzing the similarity of attributes among the nodes, packet drop detection, and quantity of successful transmission of packets by the nodes. Hence, a reliable and secure routing path is chosen for data transmission by the proposed BSCSRP protocol. However, the proposed BSCSRP protocol suffers from high routing overhead that may degrade the network performance.

In future works, we aim to reduce the routing overhead to make the BSCSRP protocol more efficient. This may further enhance the network lifetime. Moreover, the optimal route can be selected by a meta-heuristic optimization algorithm to improve the security and reduce complexity in the WANET.

Funding

There is no funding for this study.

Ethical approval

This article does not contain any studies with human participants and/or animals performed by any of the authors.

Informed consent

There is no informed consent for this study.

Authors' contributions

All the authors have participated in writing the manuscript and have revised the final version. All authors read and approved the final manuscript.

Declaration of Competing Interest

Authors declares that they have no conflict of interest.

REFERENCES

AlFarraj O, AlZubi A, Tolba A. Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. J. Ambient Intell. Humaniz. Comput. 2018. doi:10.1007/s12652-018-0885-1.

Anwar RW, Zainal A, Outay F, Yasar A, Iqbal S. BTEM: belief based trust evaluation mechanism for Wireless Sensor Networks. Future Generation Computer Systems 2019;96:605–16. doi:10.1016/j.future.2019.02.004.

Bhushan B, Sahoo G. Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. Wireless Personal Communications 2017;98(2):2037–77. doi:10.1007/s11277-017-4962-0.

Cui J, Shao L, Zhong H, Xu Y, Liu L. Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks. Peer-to-Peer Networking and Applications 2017;11(5):1022–37. doi:10.1007/s12083-017-0581-5.

Hu L, Wang Z, Han Q-L, Liu X. State estimation under false data injection attacks: security analysis and system protection. Automatica 2018;87:176–83. doi:10.1016/j.automatica.2017.09.028.

Jeba Annlin, V S, Paramasivan B. Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks. Computers & Electrical Engineering 2013;39(6):1867–79. doi:10.1016/j.compeleceng.2013.03.019.

Kumar A, Pais AR. Deterministic En-Route Filtering of False Reports: a Combinatorial Design Based Approach. IEEE Access 2018;6:74494–505. doi:10.1109/access.2018.2883474.

Kumar A, Pais AR. In: 2019 11th International Conference on Communication Systems & Networks (COMSNETS). Blockchain based En-Route Filtering of False Data in Wireless Sensor Networks; 2019. doi:10.1109/comsnets.2019.8711352.

Kumar, A., & Pais, A.R. (2017). En-Route Filtering Techniques in Wireless Sensor Networks: a Survey. Wireless Personal Communications, 96(1), 697–739. doi:10.1007/s11277-017-4197-0

Kumari R, Sharma PK. A Literature Survey on Detection and Prevention Against Vampire Attack in WSN. Advances in Intelligent Systems and Computing 2017a:271–9. doi:10.1007/978-981-10-3770-2_25.

Kumari, R., & Sharma, P.K. (2017). A Literature Survey on Detection and Prevention Against Vampire Attack in WSN. Advances in Intelligent Systems and Computing, 271–279. doi:10.1007/978-981-10-3770-2_25

Lei L, Yang W, Yang C, Shi H, Yan H. In: 2016 35th Chinese Control Conference (CCC). False data injection attack on distributed state estimation over a wireless sensor network; 2016. doi:10.1109/chicc.2016.7554645.

Nisha AS, Vaishali V, Shivaranjani T, Subathra P. In: 2016 S International Conference on Science Technology Engineering and Management (ICONSTEM). Notice of Violation of IEEE Publication Principles: the effect of vampire attacks on distance vector routing protocols for wireless ad hoc sensor networks; 2016. doi:10.1109/iconstem.2016.7560961.

Osanaiye OA, Alfa AS, Hancke GP. Denial of Service Defence for Resource Availability in Wireless Sensor Networks. IEEE Access 2018;6:6975–7004. doi:10.1109/access.2018.2793841.

Padmaja P, Marutheswar GV. Energy efficient data aggregation in wireless sensor networks. Materials Today: Proceedings 2018;5(1):388–96. doi:10.1016/j.matpr.2017.11.096.

Patel AA, Soni SJ. In: 2015 Fifth International Conference on Communication Systems and Network Technologies. A Novel Proposal for Defending against Vampire Attack in WSN; 2015. doi:10.1109/csnt.2015.94.

Sandhya MK, Murugan K, Devaraj P. Selection of aggregator nodes and elimination of false data in wireless sensor networks. Wireless Networks 2014;21(4):1327–41. doi:10.1007/s11276-014-0859-y.

Santhosh G, Palanichamy Y. Effective Verification Scheme for Filtering Injected False Data in Wireless Sensor Networks. Lecture Notes in Networks and Systems 2018:3–13. doi:10.1007/978-981-10-6890-4_1.

Shahzad MK, Nkenyereye L, Islam SMR. A Fuzzy System based Approach to Extend Network Lifetime for En-Route Filtering Schemes in WSNs. Proceedings of the 2019 11th International Conference on Computer and Automation Engineering - ICCAE 2019, 2019.

Sreevidya B, Rajesh M, Mamatha TM. Design and Development of an Enhanced Security Scheme Using RSA for Preventing False Data Injection in Wireless Sensor Networks. Ambient Communi. Comput. Syst. 2018:225–36. doi:10.1007/978-981-10-7386-1_20.

Sulochana S, Manjula V. In: 2016 International Conference on Information Communication and Embedded Systems (ICICES). Resilient system for secure sharing of information against false data injection attack; 2016. doi:10.1109/icices.2016.7518943.

Tariq M, Khan M, Fatima S. In: 2018 International Conference on Applied and Engineering Mathematics (ICAEM). Detection of False Data in Wireless Sensor Network Using Hash Chain; 2018. doi:10.1109/icaem.2018.8536305.

Vasserman EY, Hopper N. Vampire Attacks: draining Life from Wireless Ad Hoc Sensor Networks. IEEE Transactions on Mobile Computing 2013;12(2):318–32. doi:10.1109/tmc.2011.274.

Vinodha D, Mary Anita EA. Secure Data Aggregation Techniques for Wireless Sensor Networks: a Review. Archives of Computational Methods in Engineering 2018;26(4):1007–27. doi:10.1007/s11831-018-9267-2.

Wazid M, Katal A, Singh Sachan R, Goudar RH, Singh DP. In: 2013 International Conference on Communication and Signal Processing. Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network; 2013. doi:10.1109/iccsp.2013.6577120.

Yang W, Zhang Y, Chen G, Yang C, Shi L. Distributed filtering under false data injection attacks. Automatica 2019;102:34–44. doi:10.1016/j.automatica.2018.12.027.

Isaac Sajan R was born in Kanyakumari, India, in 1984. He received his B.E., M.E., and Ph.D degrees in Computer Science and Engineering from Anna University, Chennai, India, in 2006, 2008 and 2021. Currently he is working as an Assistant Professor in Ponjesly College of Engineering, Nagercoil, India. His-current research interests include Wireless Sensor Networks, Mobile Computing, Wireless Communications in general and Artificial Intelligence. He is a Life Member of the Indian Society for Technical Education (ISTE).

Jasper J was born on February 28, 1981. He received the B.E., M.E., and Ph.D degrees, all in Electrical Engineering from Manonmanium Sundaranar University, Annamalai University, and Anna University, India, in 2003, 2005 and 2014 respectively. His-major research interest includes Artificial Intelligence, Wireless Communication in general and computational intelligent techniques.