Wireless Personal Communications (2021) 118:789–814
https://doi.org/10.1007/s11277-020-08044-0

Learning-Based Security Technique for Selective Forwarding Attack in Clustered WSN

Surinder Singh[1] · Hardeep Singh Saini[2]

Accepted: 23 December 2020 / Published online: 7 January 2021

Abstract

Selective forwarding attacks in WSN can damage many mission-critical applications, like military surveillance and forest fire censoring. In such attacks, malicious nodes most of the time functions like regular nodes, but sometimes drop sensitive packets selectively, like a packet recording the dissimilar power' activity, making it more difficult to identify their malicious intent. The current selective forwarding attack detection schemes, randomly select checkpoint nodes, available in-between nodes within a forwarding route, which are responsible for producing acknowledgments for each received packet. In this paper, the complete sets of nodes are differentiated into three different types based on their functionality as Inspector Node (IN), Cluster Head (CH), and Member Nodes (MN). The newly considered node as IN is considered to overhear all of the activities of the Cluster head, as CH is the most compromising node in the complete cluster, and in the case, if the CH is attacked then the complete cluster stops working in the network. The IN is trained based on certain rules and predefined parameters which analyses if the CH or MN is malicious or not and considers the required action. NS2 is considered for the simulation of the proposed methodology and also for the validation of the proposed work. In the proposed methodology, two different stages are considered as detection and correction, which works to tackle the attacks and also considering the system efficiency almost. As in the proposed methodology, the effect of the attack is minimized which increases the QOS and also better data transmission.

Keywords Wireless sensor network · Clustering · Low energy adaptive clustering hierarchy · Energy · Efficient · Nodes · Protocols · Sensors · Routing · Transmission · Packets

Abbreviations

r_0	Radius of the cluster
R_0	Transmission range of the network
CRV	Composite reputation range
CH	Cluster head

✉ Surinder Singh
sunny16387@gmail.com; surindersingh.phd@gmail.com

[1] Research scholar, IKG PTU Jalandhar, Kapurthala, Punjab, India

[2] Professor, Indo Global College of Engineering, Abhipur, Punjab, India

IN	Inspector node
MN	Member node
$node_{id}$	Identity of any node
a	Constant
Pr_{id}	Forwarding rate
b	Constant
E_{else}	Surplus energy of the node
E_0	Initial energy level of the node

1 Introduction

Wireless Sensor Network (WSN) is the combination of various sensors integrated for different tasks and purposes and are rendered or separated by distance or a location. Figure 1 shows the architecture of WSN. Sensor nodes are used for information gathering and also for the transfer of the considered packet back to the destination in the network. The base station is the node which is a bit different from the rest of the nodes as it is having high energy-related resources, high computational power, and also strong communication power, following proper information processing and collection [1]. WSN is used in several other sectors, Such as in applications for military, medical, landslide detection, and many more [2–10].

1.1 Routing Protocols in WSN

The routing protocols [11] in WSN are as follows considering the concept of routing:

1.1.1 Data-Centric Protocols

In this type of routing protocol, messages are shared by the base station to a defined area, and the base station keeps on looking for the data. SPIN protocol, for example, falls under that category. In this routing, processing's like Flooding and Gossiping is used. Both the SPIN and the directed diffusion are considered for data-centric protocol- the aggregated data are considered for data sharing. Sensor Protocols for Information through Negotiation (SPIN) uses a naming method for representing the information gathered. Conversely, node

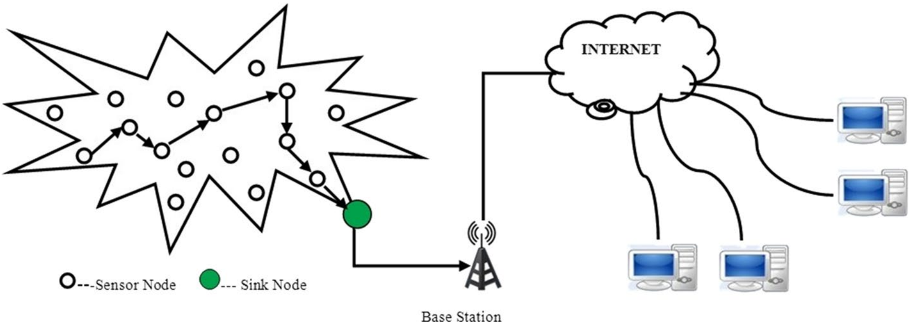

Fig. 1 The architecture of wireless sensor network [38]

mobility will challenge the SPIN model's speed and adaptability. In guided diffusion, the sinks ask the sensor node data by transmitting the message as the request. The major issue in the case of the data-centric technique is as it is best suited for the static type of network rather than for the dynamic networks or for the network where the nodes are mobile (free to move).

1.1.2 Hierarchical Protocols

Clustering in WSN is defined as the group of different nodes integrated into a group. From the available nodes in a cluster, a node is considered as the cluster head, which is responsible for the data gathering from all of the other nodes in the cluster and sharing the same with the base station. IN other terms clustering is also defined as the energy-efficient protocol. The major goal to consider the collection of nodes as a cluster is to minimize the energy consumption by defining the well-suited paths for the data transmission, also the clustering helps to maximize the lifetime of the sensor nodes. Clustering is best considered for load balancing between the communicating nodes. In many of the clustering techniques like LEACH, TEEN, APTEEN, and PEGASIS where the nodes which are having higher energy usage are considered as the cluster head and are answerable about the inter-cluster communication and also for intra-cluster communication. The shortest path technique is used for the selection of the shortest path for the transfer of data packets within the source and destination. As in the case of clustering-based networks, the time consumed is more because of the selection of the cluster head because of which they are not well-suited for the applications where the time is considered as the critical factor.

1.1.3 Location-Based Protocols

Use location information for energy-efficient routing. Some location-based protocols are MECN, SMECN, GEAR. Multi-hop routing in WSNs offers little defense for identity deception by re-providing routing data, as multiple in-between nodes are used to reach the destination. WSN's multi-hop routing becomes often the target of malicious attacks. Efficient routing protocols have been used to protect the WSN from harmful attacks.

Nowadays, WSN is among the major current research domains, and just because the wireless medium is used for communication which is easily accessible and makes them favorable for the several types of attacks [11].

1.2 LEACH (Low-Energy Adaptive Clustering Hierarchy)

Low-energy adaptive clustering hierarchy (LEACH) [12] is an energetically efficient hierarchical routing protocol for WSNs operating in different rounds [13]. Each round in LEACH is considered in two different stages, i.e. the stage of setup and the stage of steadiness. Sensor nodes are grouped into clusters during the setup process, while sensor nodes share data messages to their cluster heads (CHs) in the steady process, and these CHs are responsible for communicating with the base station (BS). CH's send aggregated messages to the BS. Sensor nodes consume less energy when communicating with other nodes while consuming more energy while sending messages to the BS. Therefore, LEACH reduces energy consumption by working in two phases and rounds. The node structures itself into a local cluster in the LEACH scheme and one node acts as the head of the local cluster. LEACH requires a randomized rotation of the head position of the high-energy cluster to rotate between the sensors. These characteristics make the network with a balanced distribution of the power usage to all the nodes and allow the entire network to have a longer life. Like most other routing protocols, LEACH still lacks the safety aspects and is exposed to different types of threats [14–19].

1.3 Attacks Possible on LEACH

Attacks are nothing but the base station's prevention of getting entire and accurate sensing data, especially serious for WSNs. Most secure routing protocols based on topography resist sinkhole attacks up to a definite level. The Group of sensor nodes tracks their neighboring's unremittingly forwarding the sensing data to a sink node or base station.

LEACH protocol is considered for many types of attacks that in large measure, lower its performance. Below are the major LEACH attacks [20]:

1.3.1 Sybil Attack

Such type of attacks is majorly counted in the peer-to-peer type of networks. In this type of attack, the identity of the genuine node is trapped by the malicious node. As in the case, when two nodes are in communication then the third malicious captures the communication in between and tries to dictate others as a legitimate node, like the one with which the information is exchanged. An opponent can take all the information in this way.

1.3.2 Selective Forwarding Attack

This type of attack is over the network layer which is also termed as the Gray Hole attacks, in this, the malicious node drops the data from the complete and shares some data to the destination. Because of the data loss, the QoS degrades in WSNs. It's very difficult to detect this type of attack [21].

1.3.3 HELLO Flood Attack

To assure its presence, many of the protocols consider sharing the hello messages to the rest of the nodes which are taking part in the communication. In the case of the attack, the malicious nodes keep on sharing the hello packet to the rest of the nodes just to increase the power consumption in receiving these messages of high signal strength. The attacker node's main intention is to increase traffic within the network which also leads to collision [22].

1.4 Selective Forwarding Attack

The selective Forwarding Attacks was initially introduced by Karlof and Wagner [23], the defined type of attack is also termed as Gray Hole attack. In this type of attack, the compromised nodes just drop or refuse to forward the data packet to the other node in the network.

Selective forwarding attacks can be available in several forms as the attack can consider a single node or group of the node for dropping the data passing through them, because of which the DoS conditions arise over the single node or group of the node.

In the case when all of the packets are dropped from the malicious node then the attack is termed as the blackhole attack. In another case, the malicious node will forward the data packet to some other route just to dis-guide the routing. The selective forwarding attack in an aspect is also termed as the Neglect and Greed attack, where some of the nodes refuse to consider the route for the message as per the routing protocol [24]. The attack keeps on be part of the communication and keeps on sharing the receipt to the sender as acknowledgment for the shared packet, which is being termed as the incompetent node. The malicious node is also termed as selfish, as sometimes it just avoids its messages also.

Figure 2 illustrates a basic example of how a selective forwarding attack works. The selective forwarding attack can happen in several ways in the relation between node S and node A. Node S forward or shares the data packets to its neighboring node A, but node A stop redirecting the data packets from node S in the sink path. Else, node A can forward the packet through a high-quality eavesdropping route to an unknown malicious node. Blind Letter attack [25] is a different type of attack and is the type of selective forwarding attack wherein the complete process the malicious node ensures about the attacked node, as the neighboring node of the next hope to which the relaying packet is to be forwarded.

2 Evaluation Criteria for Secure Clustering in WSN

In the segment below the different criteria which are used for the evaluation of the clustering on WSN are described for better understanding the attacks and techniques and also for the better evaluation of the performance of the defined schemes.

2.1 Completeness

Secure clustering is a step-by-step procedure in which security priorities, i.e. confidentiality, integrity, and availability, must be guaranteed at each step. There are two stages to this process: cluster generation and transfer of data. The cluster generation phase begins with the creation of clusters, where the cluster heads (CHs) are decided and nodes are allocated to the CHs. The next step, i.e. data transmission, is aimed at protecting the data collected while its transfer from nodes towards the base station. The defined process is having two different stages: data aggregation and base-station routing. Data aggregation is the method of data transfer within the cluster via nodes into the CH. CHs then forwards the data packets towards the base station via a defined route termed as the routing method. The base station eventually receives the data packets and evaluates the value, and then the cycle will restart as depicted in Fig. 3. These measures shall be implemented to achieve stable clustering. Within this paper, the current safe methods of clustering are evaluated

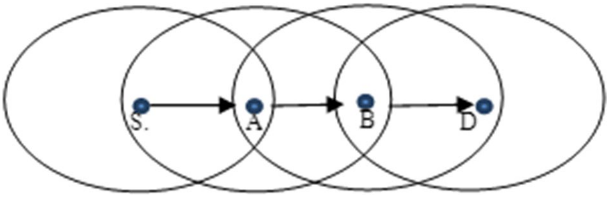

Fig. 2 Example of selective forwarding attack

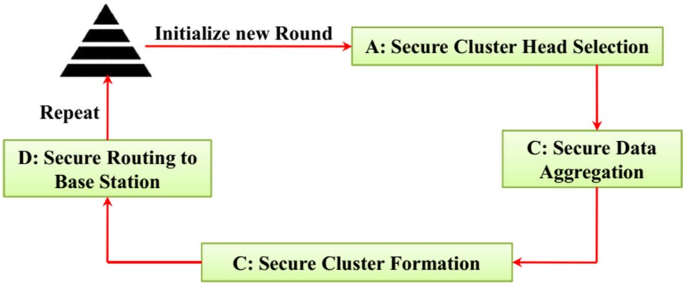
Initialize new Round
A: Secure Cluster Head Selection
C: Secure Data Aggregation
C: Secure Cluster Formation
D: Secure Routing to Base Station
Repeat

Fig. 3 Secure clustering process

and demonstrate the degree of involvement for every technique. S–CH, S–CF, S–DA, and S–DR respectively are used to represent the four different stages.

2.2 Achieving Security Goals

Secure clustering techniques are supposed to attain safety goals, i.e. integrity, confidentiality, availability, and freshness to prevent as often as possible attacks and threats. One can summarize these targets as the following [26].

2.2.1 Integrity

Data in transit is supposed not to be manipulated and actions are required to ensure that data cannot be changed/updated by unauthorized parties. A technique such as a hash function can be used to ensure that the data reaches the intended recipient without any modification.

2.2.2 Confidentiality

Confidentiality protects the critical/important information from entering the unauthorized users, thus ensuring that the correct party will access the information. And, when transmitting the data in the network, nobody other than the intended recipient will understand.

2.2.3 Availability

Availability includes the use of WSN properties, i.e. data, for approved parties, i.e. Reasonable CH and base station, are not secured during this process. This is a major goal to ensure WSN is operating efficiently and service is not refused by approving parties when they request this. Therefore, a network's usability capabilities will still be accessible even in the case of internal or external attacks.

2.2.4 Freshness

Freshness is a core aim that is compromised by replay type of attacks where the intruder broadcasts an old message to consume device resources or confuse the recipient, i.e. base station. Also, it means no repeat of old posts.

To test every current clustering technique from a robustness point of view, two notations are used as P–R and A–R respectively to show their function against the passive attack and active attack.

2.3 Robustness

A stable algorithm for clustering should be as highly robust as possible. The degree of robustness is calculated by the number of attacks impeded by the techniques. It also depends on the type of attack, whether it's active or passive. Various techniques are available to validate the robustness of each of the stable clustering algorithms against a wide range of defined attacks.

2.4 Efficiency

The safe clustering technique should consider the different limitations of the WSN resource, i.e., the size of the sensor memory, the energy, and the power of computation. It relates to avoiding the complicated security processes that could decrease the lifespan of the network. It has to align the security issue with the efficiency of the network. This refers to the Safe Clustering Algorithm performance. The efficiency of the stable clustering algorithms will be evaluated using three criteria: necessary memory (M), energy consumption (E), and processing time (P).

2.5 Dynamic Clustering

After each round, the dynamic clustering mechanism aims to reform the network structure as per the modified status and features of the sensor nodes, i.e. the remaining energy of each sensor. The static clustering techniques on the other hand allow only the updation of CH after every phase. This forms the network structure in the initial round to a fixed collection of clusters, and renders this unchangeable till the network is inaccessible, i.e. all nodes use their resources.

So there is a need to define a simple solution that enables the complex cluster network to be protected during consuming as little energy as possible and suited to low computing power. Many of the researches address the current secure clustering schemes according to past criteria and proposes a comprehensive protection scheme for routing data between sensor nodes, CHs, and the cluster-based WSN base station.

3 Review Related Works

Since Karlof initially proposed the selective forwarding attack [18], many schemes have emerged for the detection of it. Considering the traditional form of the clustering technique, LEACH, Semantic, and Abhijit [27], presented a technique for the detection of the selective forwarding attack, where a counter is being considered along with the base node. The major focus of the counter is to check whether the data packets reach the CH and at the same time, the data packets are transmitted to the destination. Depending on selective time-varying flooding tests, a node is checked by the next reliable node. Once the tests fail, the node is considered compromised. In this scheme, CHs are detected by the base station.

But this technique can be used for small-scaled WSN based clusters. As with the rise in the number of nodes, the flooding test would send more data packets than ever before to nodes. Lastly, too much energy consumption testing, itself will produce serious results for the entire network. Additionally, ignoring the quality of the channel, this technique considers normal nodes to be compromised for the bad quality of the channel.

Liu et al. [26] presented a routing technique that relies on active trust and also considers active detection. The presented technique is having high scalability, routing, security, and expectations. The active system presented in the work just senses out the malicious node in the network and makes it unavailable in the complete routing. The technique is having high efficiency and also the energy consumption is very less, as it considers fewer energy for the generation of different routes. In the work a safe and scalable technique is being presented which actually preserves the data packets from attacks using the two-stage security mechanism and also dual assurance method. Both the methods relied on active trust, where the data and the nodes are protected from many types of attacks, like blackhole and selective forwarding attacks. Das et al. [28] have considered a Genetic Algorithm for the dynamic management of the clusters head where the separation between the nodes is considered and also the faith of the sensor is node is counted. In the work, the trusted path is being considered and uses trust and CS algorithm to provide secure routing paths.

Sharmila et al. [29] implemented a lightweight detection method within the WSN to detect the sinkhole attack. The digest message technique was designed to recognize the attacks at the sinkhole and received very less resistance to collisions. To detect the sinkhole attacks the methods for the digestion of the data are broadcasted using the trusted path and also the process varies, from the actual nature of the system. As the presented technique considers the active trust mechanism by which various types of attacks are detected like blackhole and selective forwarding attack. Karlof et al. [30] have presented a work towards the security in the WSN, as per the literature, many of the techniques have considered security as the major concern. Based on the research gap counted by the author many of the security goals are considered in the works presented for routing in WSN, it has created many possibilities to attack ad-hoc and also peer-to-peer networks are considered against powerful attacks concerning the sensor network. Already, two types of attacks on sensor networks, known as sinkholes and HELLO Roods, have been suggested by the researchers.

In order to find and monitor the various attacks in WSN like selective forwarding attacks, Alaimi et al. [31] presented a detection technique for the selective forwarding attacks and also have considered different techniques for network monitoring. The defined technique is capable to detect the attacks over the network layer without considering much of the efforts. For the type of attack defined in the work, the compromised node starts working as some other node in the system, and also the malicious node can drop some of the private data before sharing the same to the destination node. In the proposed technique two-stage security mechanisms is considered and also count the dual assurance technique. Geethu et al. [32] proposed a system for the transmission of multipath. The built-up system was used against selective forwarding attacks as a defense technique. In this system, if at the time of routing a node could feel a packet drop, then the packet is forwarded over an alternative route. The reliability of the routing technique was optimized because of the resending technique. The described technique safeguards the network from many forms of attacks, like black hole attack, and limited, active trust-based forwarding attack.

Motamedi et al. [33] developed unmanned aerial vehicles (UAVs) to locate black hole attacks within WSN. A weak node in blackhole attack, that could reveal the shortest and most feasible route to the destination, draw more network traffic, and drop all the data packets. The authors had developed a method to solve this issue in the shortest possible time; the node which is having the probability of being attacked is detected. The technique is being used for the verification of the network nodes and also to avoid the malicious nodes, the Sequential Probability Ratio Test method is considered as a dynamic threshold system. In the presented technique the compromised node is detected with the help of a DP-designed two-system security mechanism and trust. A security method was implemented by Latha et al. [34], utilized for finding the routing path as safe, and also considered to search authenticate sensor nodes. But the protected node cannot be transmitted when implementing this technique for the real world, even in an active device. It provided the possibility of upgrading the system to a few of the features.

Mezrag et al. [35] developed a trusted and stable routing scheme that uses a two-stage authentication technique and a dual assurance mechanism to pick the node and protect the WSN data packet. All techniques relied on the Active Trust to secure many forms of attacks during routing, like black hole attack, and selective forwarding attack. The major goal of the work was to establish a trustable secure routing technique for clustered WSNs and to present a technique consisting of an active detection routing protocol and data routing protocol that reduces the possibility of selecting malicious nodes or attacked nodes as shared nodes. The presented technique aims to optimize the lifetime of sensor nodes by distributing the data packets in a better direction. A protocol is proposed to find the trustable route from source to destination for the WSNs to effectively attain this objective. The source node is then gen- deleted, as the network transfers the data packets from source to destination. Using elliptic curve cryptography (ECC), the transmitted data is encrypted. This proposed scheme will easily classify highly energy consuming, malicious nodes in the network. Ultimately, avoiding black holes and selective forwarding attacking is achieved via the discussed secure routing system, which upgrades the packet transmission ratio. The framework suggested offers numerous characteristics that are considered in WSN's real-time applications. For example, it has higher precision, minimal loss of energy, ease of use, privacy, and reliability.

Jeba et al. [36] in this work author has defined a novel technique for safe data communication in cluster-based WSN (HCBS) which relied on the well-known LEACH routing protocol called Hybrid Cryptography-Based Scheme. As a multi-constrained solution to the requirements, HCBS is based on a combination of Elliptic Curves based cryptography technique to exchange keys using symmetric keys for data encryption and MAC operations. The results obtained after a series of tests on the TOSSIM simulator showed that our proposal achieves good output in terms of energy consumption, loss rate, and end-to-end latency. Furthermore, HCBS guarantees a high degree of protection. This protocol is based on a combination of two main approaches; cryptography based on Elliptic Curves introduced for key exchange and cryptography based on the symmetric key for data encryption and MAC operations; the suggested procedure seems to strengthen the safety of the LEACH ensuring the basic safety criteria. So, it can be resilient against attacks, sometimes waged against LEACH. The author evaluated HCBS efficiency in terms of energy consumption (communication and computing costs), failure rate, and end-to-end delay using a collection of simulations and comparisons with SecLEACH. Findings have shown that the overhead produced by HCBS is nearly low compared to SecLEACH's. Additionally, HCBS enables the EED to be stable, even though the number of nodes in the network increases.

In [37], Sundararajan et al. have deployed uniformly in WSN to transfer the data gathered by the sensor nodes periodically. The WSN network layer's main threat is still sinkhole attack and it is a major challenging problem for sensor networks, where the malicious node drops the data packets from the other usual sensor nodes and loses the packets. A method for detecting the intruder in the network using Low Energy Adaptive Clustering

Hierarchy (LEACH) protocol for the various routing processes is used in this research. Within the proposed technique, the IDS agent measures the intrusion ratio (IR) using the detection metrics, like the number of packets transmitted and received. The numeric or non-numeric measured value shows natural or malicious operation. As the sinkhole attack is detected, the IDS agent alerts the network to stop the transmission of the data. To make it immune to the weak sinkhole attack. The outcome of the simulation shows that the weakness like sinkhole attacks on LEACH loses all the packets transmitted through the CH. With minimal computation, the proposed IDS captured the sinkhole nodes and alerted the usual sensor nodes. As the calculation of the proposed IDS is simple, it requires less energy, Furthermore; the numerical analysis shows that the proposed IDS can achieve minimum overhead computation and lower energy consumption.

4 Issues and Challenges

The most important issue that comes across is the usage of energy. The amount of energy consumed is very high. Thus, it has become one of the big problems for the WSN structure. This is not only because of the usage of sensor nodes but also of the important effects on the views of green computing. The clustering technique is very essential and plays a prime role in WSN. It has many advantages such as improvement in bandwidth and its usage, decreases the time taken and also reduces wasteful energy consumption. As everything has it is good and bad in the same way this technique has some loopholes and these are as follows:

4.1 Throughput

It is accepted to provide some better solutions for improving the quality of services offered to the consumers involved in a network, the analysis for noting the solidity in the codeless network. The most critical situation in WSN arises while sharing the data. On the other hand, problems related to WSN plays a vital role while transmission of data, so that the abilities of WSN can get extended. However, this results in lowering down the capabilities and abilities and also delays in output.

4.2 Energy Efficient Design

There are two types of issues related to WSNs. The two different issues are: depletion of energy and the other is extending the working status of the networks. The batteries of WSN have a short life span and it cannot even think of replacing it and nor it can be revitalized. The usage of energy is very high with respect to the elements of sensor nodes whether it is in working or stable form. The energy used by the inactive nodes can be saved by applying such techniques of saving power. We can switch off the switch when nodes are at non-participating mode.

4.3 Energy Saving in Meddling Environment

In a wireless environment, nodes go with an adverse situation. It might get affected by these activities. Thus, framing many other ways for the utilization of power can be reduced.

4.4 Message Sharing

The important role which WSN plays is the transferring of data and sharing of information. Hence, there are many other ways of delivering information with the desired sensing nodes in WSN. With the use of packets, the data can be shared with the appropriate and desired nodes. If the data shared is not delivered to the nodes then it might affect the performance of the data transport and increases the energy used. Hence, the level of delivery should be high.

4.5 Network Lifetime

The energy level can be lower down in the same or other cluster making use of an effective clustering approach and results in long-lasting networks. In the field of commercial and manufacturing aspect; the consumption of energy is such a big challenge.

4.6 Limited Power

The very small and less powered batteries are used in Nodes i.e. why it has a limited ability to store energy when used in networks. Thus, the energy amount is limited so; it is observed to follow an effective method. And the energy used can be reduced by clustering arrangements.

4.7 Scalability

Many sensor nodes get the break down because of the inappropriate infrastructure in WSN. It has expanded in a few areas. In this situation; routing protocols with higher abilities are used so that a ton of nodes could be used. There are various small nodes. Sensor networks cannot store large information as it is very difficult for them to do that.

4.8 Data Aggregation

Data aggregation is used for sharing info that might be useful and can eradicate the information that is not needed with the help of WSNs. It is useful in decreasing power wastage. It helps in collecting the data and information that is required for enhancing the lifeline of the networks.

5 Authors' Contributions

In the majority of the defined techniques, the major contribution is towards the authenticated data sharing and detection of the attacks in the cluster network, while the untouched or fewer works are available that works towards the formulation of the problem caused by the attack. The main contribution of this paper is to propose a Learning-Based Security Technique for Selective Forwarding Attack in Clustered WSN. In the presented technique, the complete set of nodes are differentiated into three different forms as Cluster Head (CH), Inspector Node (IN), and Member Nodes (MN), where the IN is supposed to track each of the activities of the member nodes and CH. The IN is trained based on certain rules and the data is gathered for the available network based on the defined rules which are then used for the identification of the malicious activity by the MNs or CH. After detection of the attack, the CH is updated with updating the routing protocol, and also in the case of the MNs the routing is updated to keep on the data transmission.

6 Materials and Methods

After considering the different techniques available for network security and based on the literature considered, it is quite clear that there still exists a gap to be considered for further consideration in the case of the cluster-based networks. In the case of the cluster-based WSN, the most hurdle part is in the case when the CH (Cluster Head) is compromised because of which the complete network goes down. In the work presented the forwarding type of attack is being considered where the attacker grabs a specific node and drops the data packets while transmission phase, like creates a black hole in the network.

In the cluster network the available nodes are considered of three different types as CH (Cluster Head), IN (Inspector Node), and MN (Member nodes), which are isomorphic. The radius of the cluster is almost half of the communication range of the network so that two nodes from a specific network can communicate with one another, as:

$$r_0 = R_0/2 \tag{1}$$

where r_0 is defined as the radius of the cluster and R_0 is the defined transmission range of the network.

In the network, the CH and IN are decided based on the Composite Reputation Value (CRV), by which the node with maximum CRV act as a CH and the next node act as IN, and the computation is based on the forwarding rate and energy level of the nodes, the mathematical formulation of the CRV is as under:

$$Val\left[node_{id}\right] = a * \Pr_{id} + b * \frac{E_{else}}{E_0} \tag{2}$$

where a and b are the defined constants which range as $0<a,\ b<1$, and also $a+b=1$, E_0 is the initial energy level of the node, E_{else} defines the surplus energy of the nodes, $Val\left[node_{id}\right]$ is the CRV for the specific node, $\Pr_{id}$ is defined as the forwarding rate for the defined node.

In this work a novel technique is presented which is having some predefined special types of nodes as, an inspector node (IN), which is being used for ensuring the security in the cluster-based networks. In the research methodology, three different types of nodes are defined within a cluster as Cluster Head (CH), Inspector Node (IN), and Member Nodes (MNs) as depicted in the figure below. The radius of the cluster is defined as half of the transmission range of the network so that member nodes of the cluster can communicate with one another. IN is being used to keep track of all of the activities of the CH and also tracks the behavior of the CH to detect the malicious activity of the CH and also of the other nodes too. The CRV is being used to define the CH and IN inside the cluster as the node with maximum value is defined as the CH and the second maximum node is considered as the IN and the same is updated when the IN detects any of the malicious activity. The IN node keeps overhearing the CH and other MNs and also verifies for the malicious activities by the CH and updates the same in the routing table in the case when any of the malicious activity is being noticed.

The functionality of the nodes defined as IN, MN, and CH is quite different as:

6.1 Inspector Node (IN)

In the case of the cluster-based WSN, the cluster head plays a vital role in the overall communication system and if the CH is compromised then the complete system will get affected as in most of the transmission it acts as the relay node. The IN is being used to overhear all of the communication by or through the CH and also keep the track of the communication of other member nodes, the IN maintains a transmission table which is having some predefined parameters based on which the IN is trained and the same parameters are defined in the transmission table of the IN which updates on every successful and unsuccessful transmission. The parameters are as Loss in Data, Delay time, Time to react, response time, etc. And in the case when the IN detects any of the malicious activity then it just broadcasts the same in the network and updates the CH in the routing table and transmission table. The set of rules used to train the IN are as under:

1. *Reception and delay rule* The sink should receive all of the data packets from all of the member nodes and cluster head within a specific time out, else condition of this will define an occurrence of the attack.
2. *Sub-list of cluster head member's rule* The CH should have the complete list of member nodes via the first packet shared and found missing then the indication is for an attack.
3. *Information loss rule* At the start of the communication the CH shares a control packet to the sink which is having specific information about IN and MN and it should be ensured that the required data about the MN is shared and is available otherwise there is malicious activity.
4. *Time to react/response time rule* The In should record the response rate of the CH and member nodes and if any odd symmetry is noticed then make all necessary actions required after detection of the attack.

6.2 Cluster Head

As already mentioned the cluster head is having a key role in the overall communication in the case of the cluster-based WSN. The CH is responsible for communication at levels 1 and 2 and in the case when the CH is compromised then the complete cluster goes down.

6.3 Member Node

Member nodes are responsible for data transmission and gathering of the same and also are supposed to update itself for various energy requirements other network-related requirements. MN is being used to compute the CRV value of each node which is well used to define the CH and IN.

6.4 System Architecture

The defined techniques work towards the detection of the attacks or detection of the malicious nodes and also try to work towards the resolution of the same. In the work, a training system is being used for training the IN based on some pre-defined set of rules which are formulated based on the various network performance-related parameters. The major aim for the induction of the IN in the cluster is to detect the malicious activity of the CH, and in the case when the CH is compromised and detected by IN then the routing table is updated and the IN for the current communication works as the CH and also broadcasts about the malicious activity to rest of the cluster. After the completion of the current communication, the IN goes for the computation of the CRV in the cluster to update the CH and IN as new. Figure 4 illustrates the architecture of the proposed method.

Below are algorithmic steps for the proposed methodology which considers all of the defined parameters and actual visual network for transmission and security in the same.

```
Step 1: $N_i = (1, 2, 3, 4, ........, k, ......., n - 1, n)$, // is the No. of clusters in a network.
Step 2: $C_i H \rightarrow$ cluster head of ith cluster,
Step 3: $I_i N \rightarrow$ is the inspector node for ith cluster,
Step 4: $\mathrm{M\,N_i} \rightarrow (\mathrm{m_1, m_2, m_3, \ldots\ldots\ldots, m_l, \ldots.., m_l})$,
Step 5: if $M N_{ij}$ is looking to establish communication with $M N_{kl}$.
Step 6: $M N_{ij}$ will transmit towards $C_i H$ and then to $I_i N$,
Step 7: $I_i N$ verifies the rules based on $R$,
Step 8: If no malicious activity found then proceed as $C_i H \rightarrow C_k H \rightarrow M N_{kl}$.
Step 9: $I_k N$ verifies for any malicious activity on the basis of the training data available,
Step 10: If ok then proceed $C_k H \rightarrow M N_{kl}$,
Step 11: Else define $C_k H$ as malicious and take all required actions,
```

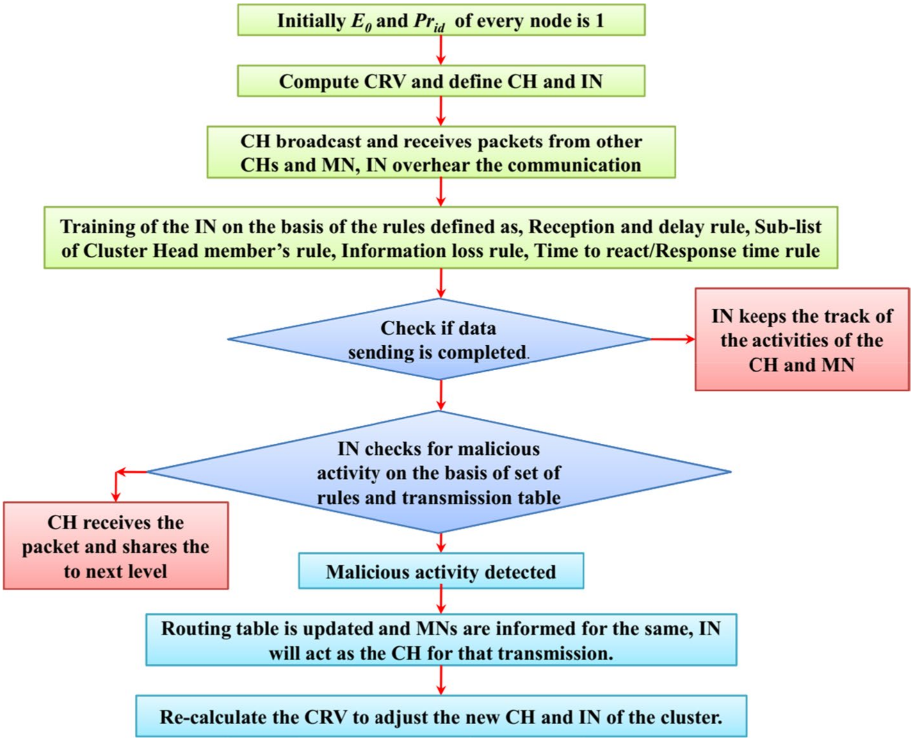
Initially E_0 and Pr_{id} of every node is 1
Compute CRV and define CH and IN
CH broadcast and receives packets from other CHs and MN, IN overhear the communication
Training of the IN on the basis of the rules defined as, Reception and delay rule, Sub-list of Cluster Head member's rule, Information loss rule, Time to react/Response time rule
Check if data sending is completed.
IN keeps the track of the activities of the CH and MN
IN checks for malicious activity on the basis of set of rules and transmission table
CH receives the packet and shares the to next level
Malicious activity detected
Routing table is updated and MNs are informed for the same, IN will act as the CH for that transmission.
Re-calculate the CRV to adjust the new CH and IN of the cluster.

Fig. 4 Working architecture of the research methodology

Step 12: $I_k\,N$ becomes $C_k\,H$,
Step 13: $C_k\,H$ transmits the data to further level,
Step 14: Select $I_k\,N$ from C_k,
Step 15: Else, $C_i\,H$ is malicious,
Step 16: $I_i\,N$ becomes cluster head,
Step 17: $C_i\,H$ transfers for further level,
Step 18: Select $I_i\,N$ from C_i.

7 Result and Analysis

The work presented is for the detection and resolution of the selective forwarding attack in the cluster-based WSN, the complete methodology is simulated in NS2 and the work is validated based on certain performance-related parameters like Packet Loss Rate (PLR), Missed Detection Rate (MDR), False Detection Rate (FDR) and also the energy consumption of the individual nodes is being considered.

In the proposed methodology (in Fig. 5) the complete set of nodes are differentiated as member nodes (MNs), cluster head (CH), and inspector node (IN), where they are differentiated based on the different functionalities of the same. In every cluster, a single node is being considered as the cluster head which is responsible for all of the communication within the cluster and also outside the cluster, as shown by node 0 in the figure above. The Inspector node is supposed to overhear all of the communication in the cluster and also responsible for the malicious activity of the MNs and CH with the help of learning process defined for the same. Rest all available nodes are the member nodes in the cluster. The CH and IN are defined with the help of the CRV estimation as explained in Eq. (2).

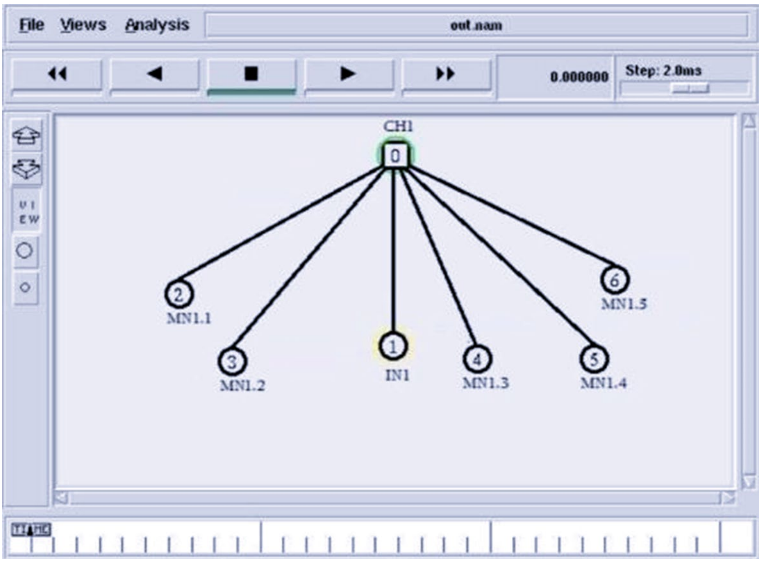

Fig. 5 Proposed system architecture

In the complete communication process, the MN1.1 is asking for data transfer to MN1.3 for which the CH should be requested for the path establishment and routing information for which MN1.1 sends a request packet to CH for further processing (as Fig. 6).

After sending the request packet the MN1.1 transmits the data packet to CH so that the data can be further transmitted to the destination node.

IN is supposed to overhear all of the communication via CH or from any of the MNs, in the current example the IN1 overhears for the ongoing communication over CH and acknowledge CH if no malicious activity is recorded based on the training rules defines which helps IN to detect the malicious activity.

After receiving an acknowledgment from IN about the ongoing communication the CH sends the data packet to MN1.3 (Fig. 7) which is a destination node in the current established communication. The data sharing is possible via the CH because which the chances to over-ride the current communication via attack is through CH and in the case when the CH is attacked then the complete cluster is somehow attacked. IN first will ensure about the current activity of the CH and then will share an acknowledgment to the CH about the same which then is followed by the further transmission of the data packet to the destination node.

Once the communication is established and data sharing is completed means the data packet reaches the destination then the destination nodes provide an acknowledgment to the CH for the completion of the communication which then informs the same to the source node and IN. In the current case, the destination node MN1.3 sends the acknowledgment to CH and CH provides the same to MN1.1. Figure 8 illustrates the Communication overhearing by IN. Figure 9 shows the data packet transfer from Ch to MN1.3. Figure 10 illustrates the successful transmission of data acknowledgement sharing. Figure 11 shows the detection of malicious activity by IN.

As per the research methodology, the complete data sharing is having two different phases as detection of the malicious activity or all good means no attack found. All the

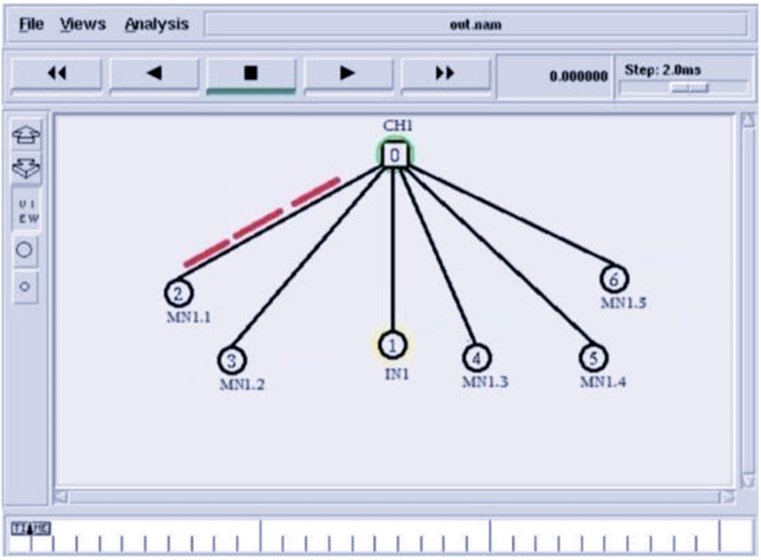

Fig. 6 Request packet from MN1.1 to CH

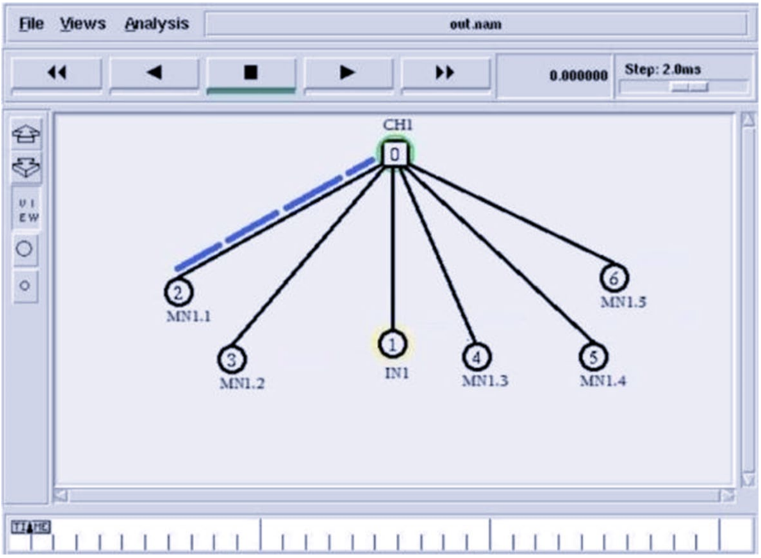

Fig. 7 Data transfer from MN1.1 to CH as defined in the proposed system

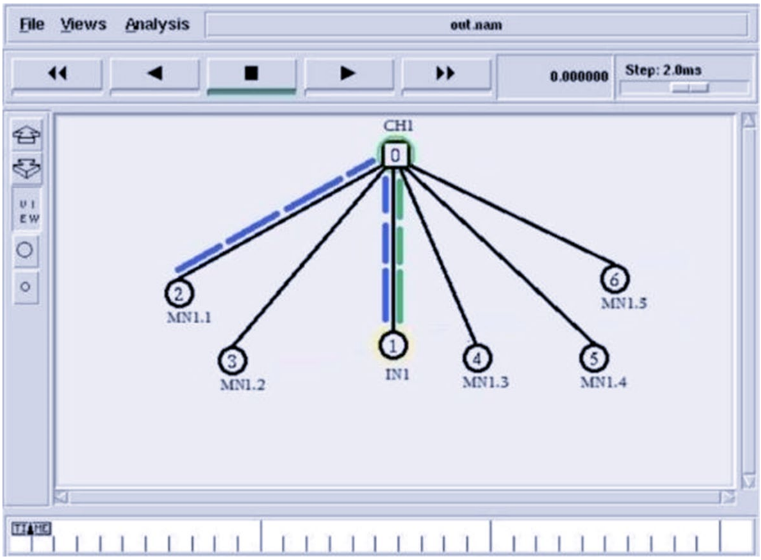

Fig. 8 Communication overhearing by IN

above processing diagrams are the example of the no attack found in the overall communication while the figure above is the case for the detection of the malicious activity over CH. The detection is confirmed based on the learning rules used for training the IN, after detection, the IN informs the same to other nodes involved in the communication and starts behaving like CH for current communication and transmits the data to the destination. The

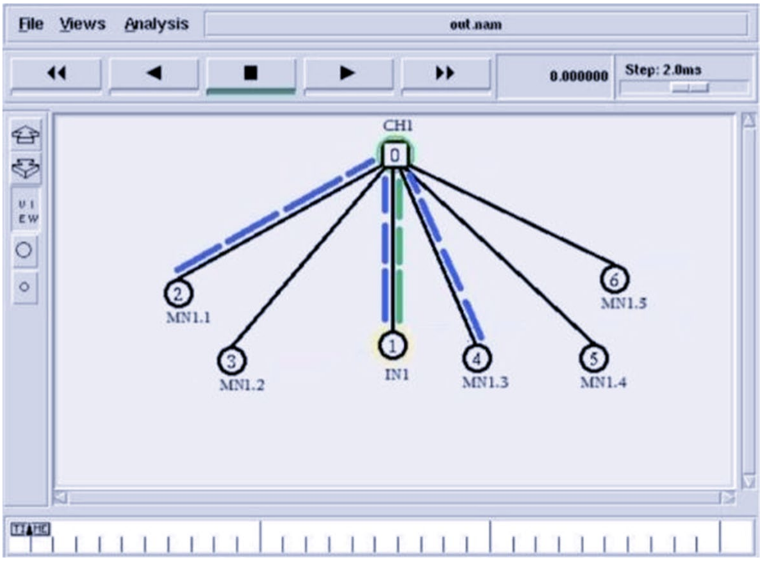

Fig. 9 Data packet transfer from Ch to MN1.3

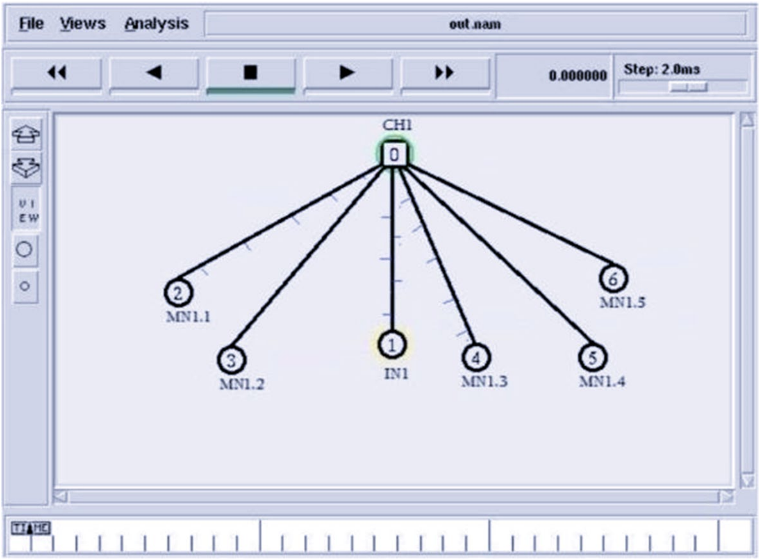

Fig. 10 After successful transmission of data acknowledgement sharing

routing table is updated based on the detection tracked and the CH and IN are re-counted using the CRV described in Eq. (2).

The graphs below present the comparison of various parameters considering various previously defined techniques and proposed methodology based on the energy consumption, delay and latency time, packet loss ratio.

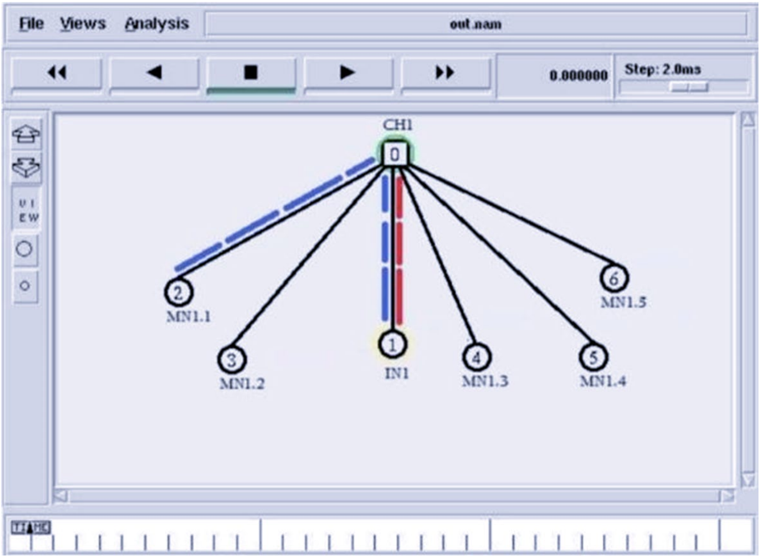

Fig. 11 Detection of malicious activity by IN

7.1 Energy Efficiency Comparison

Within this section, the findings are contrasted with current methods using the performance-related parameters like energy consumption, packet loss ratio, and latency, such as RSPA, HCBS, and proposed methodology.

7.1.1 Energy Consumption

The sensing node's energy consumption is supposed to be reduced, and the sensor nodes are supposed to be energy efficient, as the available energy supply essentially dictates their lifespan. The formula for energy consumption to submit c bit data to a distance d is expressed as under,

$$E_{Tx}(c, d) = E_{elec} * C + \in_{amp} c * d^2 \tag{3}$$

where E_{Tx} depicts the energy loss, during the data transfer, E_{elec} depicts the loss of energy transmitter, $\in amp$ is the amplifier energy, and d is the distance.

Energy consumption in WSN is a major challenge as the deployed sensor nodes cannot be charged if they losses the battery, which is also due to the region of deployment, as the WSN is being generally considered over the places where the human invention is not possible. In current work, the major focus is on the detection of an attack and at the same to reduce the impact of the attack over the network. As in the research technique, the IN node keeps the communication ON after CH is being compromised by declaring itself as CH for the current communication, the considered criteria works to reduce the energy consumption as in the case when the packet is dropped or lost after detecting an attack for which the second round of communication establishment is required which consumes the power of all

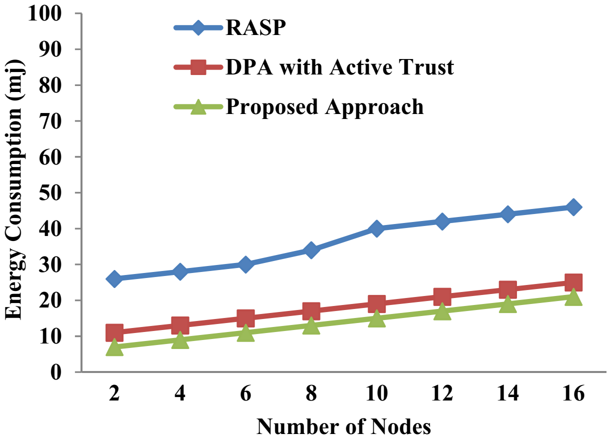

Fig. 12 Performance for energy consumption

Table 1 Comparison for Energy consumption

Network size	RSPA [28] energy consumption (mj)	DPA [27] energy consumption (mj)	LBST (proposed) energy consumption (mj)
2	26	10	7
4	28	13	9
6	30	15	11
8	34	17	13
10	40	19	15
12	42	21	17
14	44	23	19
16	46	25	21

communicating nodes. The work presented is compared with two other techniques (RSPA, HCBS) for energy consumption and there is almost 40% variations in the energy consumption as compared to previous techniques as represented in Fig. 12 and Table 1.

7.1.2 Delay/Latency Time

Latency represents the time period between the response and stimulus, or a time delay with source and the target of the physical change in the device being studied, and can be measured using the mathematical formulation shown in Eq. (4) to prevent the loss of energy;

$$latency = t_d * C + s_t \tag{4}$$

where t_d is the time of packets received at the destination, and st is the time of packets started at the source node.

Table 2 and Fig. 13 showed the comparison of the delay time for the three different techniques such as RSPA, HCBS, LBST, where LBST technique has proved a remarkable difference between the delay time over the same number of nodes. The delay time/latency is quite minimum for the case of the proposed methodology.

Table 2 Comparison for latency time

Network size	RSPA[28] delay/latency (ms)	DPA [27] delay/latency (ms)	LBST (proposed) delay/latency (ms)
2	4000	11,000	3000
4	5000	12,000	4000
6	5500	14,000	4500
8	6000	16,000	5000
10	6500	15,000	5500
12	7000	15,000	6000
14	8000	27,000	6500
16	9000	11,000	7000

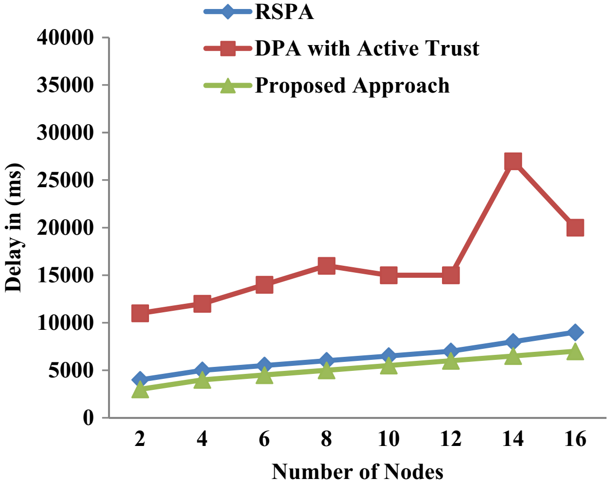

Fig. 13 Delay/latency comparison

7.1.3 Packet Loss/Drop Ratio

The PDR is predicated as documented within the trace file based on the received and generated packets. In general, PDR is evaluated as the quantitative relationship between the destination received packets and the supply packets produced. The PDR formula is determined by dividing the total number of packets at the destination, by the total number of packets produced at the source node, and then by multiplying the result produced by the percentage shown below to generate the correct outcomes.

$$PDR = \frac{t_d}{t_s} * 100 \tag{5}$$

where *PDR* is the packet delivery ratio, t_d is the total number of packets at the destination, and t_s is the total number of packets generated at the source code. Table 3 illustrates comparision performance of packet loss ratio.

Packet drop ratio highly depends on the detection rate of the attacks and also depends on the steps taken after detection of the attack or detection of malicious activities. The graphs shown in Fig. 14 are the representation of the packet drop ratio with respect to the number

Table 3 Comparison for packet loss ratio

Network size	RSPA [28] packet loss ratio%	DPA [27] packet loss ratio%	LBST (proposed) packet loss ratio%
2	8	6	4
4	9	7	5
6	10	8	6
8	11	8	7
10	12	10	8
12	14	15	9
14	15	14	10
16	16	18	11

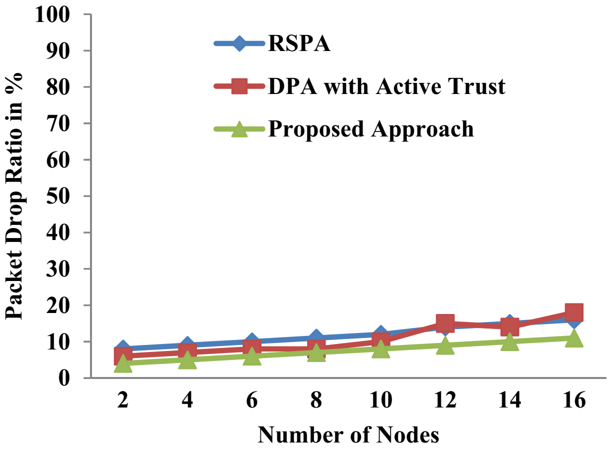

Fig. 14 Packet drop ratio comparison

of nodes where the network size is considered from 2 to 16 and also on the basis of the network size the packet drop ratio behaves differently. The packet drop ratio for the proposed technique is minimum for 4 node network and for the same number of nodes it is quite higher for other. techniques as considered for comparison for the work. In the proposed technique the packet drop ratio is around 8% for 16 node network which was and quite similar for HCBS techniques.

On basis of the results generated it is quite clear that the proposed methodology is quite efficient in terms of data loss because of the consideration of the IN as CH in the case when any of the malicious activity is detected over the CH while communication. And also, the energy consumption in the case of the proposed methodology is quite reduced but not to a large extent because the packet loss frequency in the proposed methodology is minimized which results in minimum usage of the nodes for extra transmission and communication.

8 Conclusion

Clustering is the method to group the similar type of items for better management, clustering is the technique used for data management where the data points with similar characteristics are grouped for better and enhanced management of the data. In the terms of the WSN, the various nodes are grouped based on several methods for clustering for which in the current work the clustering of the nodes is done using the LEACH method. The major issues with the WSN are the security and power conservation of the nodes which can be compromised by various types of available attacks, from which in the current work the selective forwarding attack over the WSN is being considered. In the case of the selective forwarding attack the either some part of the data packet or even the complete data can be dropped by the node in the case when the node is attacked. In clustering, the CH is the major node that acts like a master and all of the communication is via CH and in the case when the CH has attacked then the complete cluster is malicious for all of the transmissions. In the proposed methodology, the complete set of cluster nodes are differentiated as Inspector node (IN), Member Nodes (MN), and Cluster Head (CH) based on the functionalities of the nodes. IN is supposed to track the communication via CH and MNs for which training module is being considered using which the IN checks for the malicious activity by CH. The complete proposed work is simulated using NS2 and also the work is validated and compared with many of the performance-related parameters like Packet Loss Rate, MDR, FDR, power consumption, network life, etc. Based on the results presented in the above section, it is quite clear that the described methodology outperforms other techniques in terms of network lifetime, detection, and resolution of the attacks and also ensures the minimum data loss with the help of IN. In the evaluated work, very less attention is provided to various energy management-related issues which can be further elaborated in the upcoming researches.

Acknowledgement The authors of this paper acknowledge the IK Gujral Punjab Technical University, Kapurthala.

References

1. Gill, R. K., Chawla, P., & Sachdeva, M. (2016). Wireless sensor network: Threat models and security issues.
2. Sundararaj, V., Muthukumar, S., & Kumar, R. S. (2018). An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks. *Computers and Security, 77,* 277–288.
3. Sundararaj, V. (2016). An efficient threshold prediction scheme for wavelet based ECG signal noise reduction using variable step size firefly algorithm. *The International Journal of Intelligent Engineering and Systems, 9*(3), 117–126.
4. Vinu, S. (2019). Optimal task assignment in mobile cloud computing by queue based ant-bee algorithm. *Wireless Personal Communications, 104*(1), 173–197.
5. Sundararaj, V. (2019). Optimised denoising scheme via opposition-based self-adaptive learning PSO algorithm for wavelet-based ECG signal noise reduction. *International Journal of Biomedical Engineering and Technology, 31*(4), 325.
6. Sundararaj, V., Anoop, V., Dixit, P., Arjaria, A., Chourasia, U., Bhambri, P., et al. (2020). CCGPA-MPPT: Cauchy preferential crossover-based global pollination algorithm for MPPT in photovoltaic system. *Progress in Photovoltaics: Research and Applications, 28*(11), 1128–1145.
7. Rose, S. H., & Jayasree, T. (2019). Detection of jamming attack using timestamp for WSN. *Ad Hoc Networks, 91,* 101874.

8. Zhou, H., Shen, S., & Liu, J. (2020). Malware propagation model in wireless sensor networks under attack–defense confrontation. *Computer Communications, 162,* 51–58.
9. Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., & Ben-Hassine, H. (2020). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things, 9,* 100264.
10. Bhushan, B., & Sahoo, G. (2020). ISFC-BLS (intelligent and secured fuzzy clustering algorithm using balanced load sub-cluster formation) in WSN environment. *Wireless Personal Communications, 111*(3), 1667–1694.
11. Udhayavani, M., & Chandrasekaran, M. (2018). *Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: A trust-aware routing framework for wireless sensor networks*. Berlin: Springer.
12. Krontiris, I., Giannetsos, T., & Dimitriou, T. (2008). Launching a sinkhole attack in wireless sensor networks; the intruder side. In *Proceedings of IEEE international conference wireless and mobile computing, networking and communication (WIMOB '08)* (pp. 526–531).
13. Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: Analysis and defences. In *Proceedings third international conference information processing in sensor networks (IPSN '04)* (2004).
14. Bai, L., Ferrese, F., Ploskina, K., & Biswas, S. (2009). Performance analysis of mobile agent-based wireless sensor network. In *Proceeding eighth international conference reliability, maintainability and safety (ICRMS '09)* (pp. 16–19).
15. Zhang, L., Wang, Q., & Shu, X. (2009). A mobile-agent-based middleware for wireless sensor networks data fusion. In *Proceeding instrumentation and measurement technology conference (I2MTC '09)* (pp. 378–383).
16. Xue, W., Aiguo, J., & Sheng, W. (2005). Mobile agent based moving target methods in wireless sensor networks. In *Proceedings IEEE international symposium communication and information technology (ISCIT '05)* (vol. 1, pp. 22–26).
17. Jeong, H.-J., Nam, C.-S., Jeong, Y.-S., & Shin, D.-R. (2008). A mobile agent based leach in wireless sensor networks. In *Proceedings 10th international conference advanced communication technology (ICACT '08)* (vol. 1, pp. 75–78).
18. Al-Karaki, J., & Kamal, A. (2004). Routing techniques in wireless sensor networks: A survey. *Wireless Communications, 11*(6), 6–28.
19. Karlof, C., Sastry, N., Wagner, D. (2004). Tinysec: A link layer security architecture for wireless sensor networks. In *Proceeding ACM international conference embedded networked sensor systems (SenSys' 04).*
20. Perrig, A., Szewczyk, R., Wen, W., Culler, D., & Tygar, J. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks Journal, 8*(5), 521–534.
21. Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., & Kruus, P. (2004). Tinypk: Securing sensor networks with public key technology. In *Proceedings second ACM workshop security of ad hoc and sensor networks (SASN '04)* (pp. 59–64).
22. Liu, A., & Ning, P. (2008). Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In *Proceedings seventh international conference information processing in sensor networks (IPSN '08)* (pp. 245–256).
23. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures in Ad Hoc. *Networks, 1*(2), 293–315.
24. Wood, A., & Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer, 35*(10), 54–62.
25. Lee, S. B., & Choi, Y. H. (2006). A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks. In *Proceedings of the fourth ACM workshop on security of ad hoc and sensor networks (SASN'06)* (pp. 59–70).
26. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). Active trust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013–2027.
27. Semanti, D., & Abhijit, D. (2015). An algorithm to detect malicious nodes in wireless sensor network using enhanced LEACH protocol. In *Proceedings of the 2015 international conference on advances in computer engineering and applications, Ghaziabad, India* (pp. 19–20).
28. Das, S., Barani, S., Wagh, S., & Sonavane, S.S. (2016). Energy efficient and trustable routing protocol for wireless sensor networks based on genetic algorithm (E2TRP). In *Proceedings in IEEE international conference on automatic control and dynamic optimization techniques (ICACDOT), Pune, India* (pp. 154–159).
29. Sharmila, S., & Umamaheswari, G. (2011). Detection of sinkhole attack in wireless sensor networks using message digest algorithms. In *Proceedings in 2011 international conference on process automation, control and computing, coimbatore, India* (pp. 1–6).

30. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings in the first IEEE international workshop on sensor network protocols and applications, Anchorage, AK, USA* (pp. 113–127).
31. Alajmi, N. M., & Elleithy, K. (2016). A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks. In *Proceedings in 2016 IEEE long island systems, applications and technology conference (LISAT), Farmingdale, NY, USA* (pp. 1–6).
32. Geethu, P. C., & Mohammed, A. R. (2013). Defense mechanism against selective forwarding attack in wire-less sensor networks. In *Proceedings in 2013 fourth international conference on computing, communications and networking technologies (ICCCNT), Tiruchengode, India* (pp. 1–4).
33. Motamedi, M., & Yazdani, N. (2015). Detection of black hole attack in wireless sensor network using uav. In *Proceedings in 2015 7th conference on information and knowledge technology (IKT), Urmia, Iran* (pp. 1–5).
34. Latha, D., & Palanivel, K. (2014). Secure routing through trusted nodes in wireless sensor networks a survey. *International Journal of Advanced Research in Computer Engineering and Technology, 3*(11), 3792–3799.
35. Mezrag, F., Salim, B., & Mellouk, A. (2017). Secure routing in cluster-based wireless sensor networks. In *GLOBECOM 2017–2017 IEEE global communications conference*. IEEE.
36. Jeba, S. V. A., & Suresh Kumar, R. (2015). Reliable anonymous secure packet forwarding scheme for wireless sensor networks. *Computers and Electrical Engineering, 48,* 405–416.
37. Sundararajan, R. K., & Arumugam, U. (2015). Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor networks. *Journal of Sensors*.
38. Chawla, P., & Sachdeva, M. (2018). Detection of selective forwarding (gray hole) attack on LEACH in wireless sensor networks. In *Next-generation networks, advances in intelligent systems and computing*. Springer Nature Singapore Pte Ltd. (pp. 389–398).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Surinder Singh obtained his Pursuing degree in Electronics Engineering from I.K. Gujral Punjab Technical University. He holds Master's degree in Electronics & Communication Engineering from Punjab Technical University, Jalandhar passed in 2011. His total experience is 15 years, presently working as Assistant Professor (ECE) at IPR Head Chandigarh Engineering College, Mohali, PUNJAB (INDIA) since Jan-2007. His area of expertise includes Wireless communication. He has presented 13 papers in international/national conferences and published 13 papers in international journals (*SCI/SCOPUS/IEEE Peer-reviewed Journal*). He has Filled 53 Patents in the filed of Electronics & Communication Engineering.

Dr. Hardeep Singh Saini obtained his Doctorate degree in Electronics & Communication Engineering in 2012. He holds Master's degree in Electronics & Communication Engineering from Punjab Technical University, Jalandhar passed in 2007. His total experience is 20 years, presently working as Professor (ECE) at Indo Global College of Engineering, Abhipur (New Chandigarh), PUNJAB (INDIA) since June-2007. His area of expertise includes optical communication. He is author of 6 books in the field of Electronics & Communication Engineering. He has presented 76 papers in international/national conferences and published 76 papers in international journals (*SCI/SCOPUS/IEEE Peer-reviewed Journal*). He is a fellow and senior member of various prestigious societies like IETE (India), IEEE, IETI China, SCIEI USA and he is also editorial member of various international journals and conferences.