Development of Protective Scheme against Collaborative Black Hole Attacks in Mobile Ad hoc Networks

Muhammad Umar Farooq[1], Xingfu Wang[1*], Moizza Sajjad[2] and Sara Qaisar[3]
[1] School of Computer Science and Technology, University of Science and Technology of China
Hefei, 230026 - China
[e-mail: wangxfu@ustc.edu.cn]
[2] Gomal University
Dera Ismail Khan, 29220 - Pakistan
[3] International Islamic University
Islamabad, 44000 – Pakistan
*Corresponding author: Xingfu Wang

Received April 21, 2017; revised July 12, 2017; accepted November 14, 2017; published March 31, 2018

Abstract

Mobile Ad hoc Network (MANET) is a collection of nodes or communication devices that wish to communicate without any fixed infrastructure and predetermined organization of available links. The effort has been made by proposing a scheme to overcome the critical security issue in MANET. The insufficiency of security considerations in the design of Ad hoc On-Demand Distance Vector protocol makes it vulnerable to the threats of collaborative black hole attacks, where hacker nodes attack the data packets and drop them instead of forwarding. To secure mobile ad hoc networks from collaborative black hole attacks, we implement our scheme and considered sensor's energy as a key feature with a better packet delivery ratio, less delay time and high throughput. The proposed scheme has offered an improved solution to diminish collaborative black hole attacks with high performance and benchmark results as compared to the existing schemes EDRIAODV and DRIAODV respectively. This paper has shown that throughput and packet delivery ratio increase while the end to end delay decreases as compared to existing schemes. It also reduces the overall energy consumption and network traffic by maintaining accuracy and high detection rate which is more safe and reliable for future work.

Keywords: Mobile ad hoc networks, collaborative black hole attacks, aodv, owca, security

A preliminary version of this paper appeared in IEEE MSN 2016, December 16-18, Hefei, China. This version includes a comparative analysis and supporting implementation results on collaborative black hole attacks. This research was supported by the Fundamental Research Funds for the Central Universities NO. WK2150110007 and the National Natural Science Foundation of China (Grant No. 61772490, 61472382, 61472381 and 61572454).

http://doi.org/10.3837/tiis.2018.03.020 **ISSN : 1976-7277**

1. Introduction

Mobile Ad hoc network (MANET) is a self configuring network that does not need any fixed infrastructure, which minimizes their cost as well as deployment time. As each node in this network is free to move that makes the network to change its topology continuously [1]. A number of bottle necks are still hindering the secure implementation of these networks. Collaborative black hole attacks are one of the key attacks in MANETs and it swallows the entire receiving messages, similar to a black hole absorbing everything passing through it. Blocking the normal flow of the information, the attackers cripple the whole sensor network communication [2]. There are a number of solutions and methodologies reported to avert and defend against the black hole attacks [3-6]. However, these solutions are computational or energy inefficient. In the past decade, energy efficiency becomes an important study for improving the lifespan and performance of the MANETs. Significance in research of a mobile ad hoc network has been growing since last few years, due to this it is vulnerable to various kinds of security threats. Hence, secured and enhanced energy efficiency solution will be one of the key need in a present MANET technology paradigm. The aim of our research is to detect the collaborative black hole attacks in a mobile ad hoc network and it demonstrates how energy preserving model increases the efficiency of the network.

In our report, we have proposed cluster-based energy preserving detection model for mobile ad hoc networks' security against collaborative black hole attacks. This technique offers plenty of advantages for better detection and mitigation of collaborative black hole attacks. The proposed cluster-based energy efficiency model with security is implemented through Optimized Weight Based Clustering Algorithm with Security (OWCAS) alongside an energy computational model. The proposed methodology is the modified form of Ad hoc On-Demand Distance Vector (AODV) [7]. OWCAS is chosen as a base methodology for resolving the DOS attacks vulnerability. Later we have compared proposed methodology with the existing schemes DRIAODV and ERIAODV under collaborative black hole attacks in MANET. This shows enhanced results with great performance. Various parameters are considered while implementing this method such as throughput, energy, packet delivery ratio and end-to-end delay. A NS-2 network simulator is used to simulate the proposed method and assess the performance of an OWCAS and energy computation model. This simulation offers a comprehensive insight the proposed network performance under various operating conditions. This has shown a reduced energy consumption of the whole network. It has enhanced the packet delivery ratio and throughput of the network, reduced the end to end delay and save the energy of the network.

The rest of the paper is organized by the following sections, section 2 deals with the related work of black hole and collaborative black hole attacks, section 3 describes the preliminaries and formulation of the proposed work, section 4 describes the proposed methodology of detecting collaborative black hole attacks, section 5 describes the simulation setup and results, finally section 6 presents our conclusion and the future work.

2. Related Work

A number of diverse mechanisms have been proposed to prevent the black hole attacks. A complex form of black hole attack is collaborative black hole attack where multiple malicious nodes collaborate together resulting in full disruption of the routing and packet forwarding functionality of the ad hoc network during this attack [8]. AODV routing protocol does not incorporate any mechanism for security, such as authentication. That's why there is no straightforward security mechanism to prevent mischievous behavior of a specific node such as media access control spoofing, dropping packets, IP spoofing or changing the contents of control packets.

Collaborative black holes are acting in the group and prevent them from discovering the safe route. Data routing information table (DRI) is used to deal with modification and cross checking and data to identify the cooperative black hole nodes [9]. Another solution employed the powerful Analytic Hierarchy Process (AHP) mechanism to select cluster heads (CHs). These cluster heads are responsible for detection and prevention of black hole attacks [10]. For finding the authentication of the node which initiates RREP (Route Replies) message, multiple routes toward the destination node are explored, it gives an interesting solution. However, this solution is not time efficient [11].

Cryptographic techniques are some of the most prominent solution to ensure the integrity and authentication but it fail when an attacker knows the keys and use them to encrypting and decrypting the messages. This is one of the key weaknesses of this approach [12]. Black hole attacks can also be neutralized through advanced routing methods which have the best packet delivery ratio and detection probability. However, the major drawback of this technique is the higher routing overhead because the broadcasting of the packets is done periodically. The routing overhead problem resolved through reactive routing methodology but this solution suffered from a packet loss problem [13]. According to M. Wazid et al [14], the proposed tree topology helps in detection and prevention of black hole attack and it consists of router nodes, mobile nodes, and coordinator nodes. Though, this proposed mechanism works for static sensor networks but it did not consider the mobility of nodes.

If an intermediate node is a friendly mobile node, then data routing can be accomplished. Even though this mechanism defends collaborative black hole attacks, each mobile node has to maintain a large table in addition to normal data routing table that results in increased in overhead and memory space wastage. Moreover, a recently entered non malicious mobile nodes may be unfairly detected as the black hole and discarded as it might not have done any information transfer through and from the neighboring mobile nodes and it also fails in the existence of the individual or non collaborative multiple black holes since they drop further request itself, the advanced data routing information tables are used in [15-17].

Another mechanism proposed that values are randomly allotted for some parameters for each mobile node. By taking the amount of these parameters to be specific rank (a trustworthy measure), a stability factor (conversely corresponding to the velocity of a mobile node) and remaining energy consumption, trusts assessment of every mobile node is resolved. Later, each route average trust is estimated by averaging the trust of every single participating mobile node in that route and the highest average route is selected for routing. Consequently, the source node has to wait for an acknowledgment bit from the destination. If the data packet transmitted successfully, then a destination node sends back an acknowledgment bit to the source node. On receipt of confirmation from the destination node, the source node decrements the remaining energy power and increase the rank of all mobile nodes in the path. On contrary, if there is no acknowledgment bit, the source node decrements the rank of all mobile nodes in the path. Even though this mechanism handles both single and cooperative black hole attacks, all RREPs should be protected and average trust value ought to be determined. Additionally, the parameters associated with each mobile node need to be maintained and updates frequently. In order to make sure that a mobile node is malicious, it is needed to grasp up until it reaches to zero [18].

Numerous techniques have been addressed based on various criteria. They are, the routing protocol used, a Modifies routing table or not, new control packets introduced or not, a simulation tool used, performance metrics and type of black holes detected.

Table 1. Existing Schemes

Technique	Routing Protocol Used	Modifies Routing Table (Yes/No)	New Control Packets (Yes/No)	Tool	Perfor-mance Metrics	Results
DRIAODV [9]	AODV	YES	YES	NS2	Investigating multiple routes, Throughput, PDR, end to end delay	Locate safe route messages but are not time efficient
EDRIAODV [23]	AODV	YES	YES	NS2	Throughput, end to end delay, PDR	Improved PDR
DSN Based [24]	AODV	YES	YES	NS2	Throughput, end to end delay	Better Throughpu t and end to end delay
Knowledge Based [25]	AODV	YES	YES	NS2	PDR vs No of malicious nodes	Effective PDR

Table 1 presented a comparative study of existing schemes of strategies in overcoming or mitigating effects of black hole and collaborative black hole attacks on routing protocols in mobile ad hoc networks.

The key issues in previous technologies were as follows:

- To reduce the energy consumption of the mobile ad hoc network
- To increase the packet delivery ratio and throughput of a mobile ad hoc network
- To decrease the end to end delay of a mobile ad hoc network

3. Preliminaries & Formulation

This section demonstrates three issues. First, the assumptions and symbols used in this work. Second, the energy computational model. Third, the essential definitions used in this work.

3.1 Assumptions

We assume the following properties about the network model. In this network $\mathbb{N}$, the sensing tasks and data reporting are periodic. The mobile nodes are deployed in a rectangular field using zigzag model. The mobile nodes are heterogeneous (i.e., have different capabilities for sensing, processing and communication). All mobile nodes have unique ID. The mobile nodes transmit data to its immediate cluster head within the allotted time slots. A node $n_i \in \mathbb{N}$ is located in (x_i, y_i) while the position of the sink node n_b is fixed and located in (x_b, y_b). Each node can directly communicate with the sink node. We assume that mobile nodes are randomly divided into cluster by using Optimized Weight based Clustering Algorithm

(OWCA) [19]. All nodes are energy constrainted and perform similar task. We also assume that the selection of cluster head based on the minimum combine weight as mentioned below.

$$W_v = w_1\Delta_v + w_2 D_v + w_3 M_v + w_4 T_v + w_5 E_v + w_6 BS_v \tag{1}$$

where,
$w_1 = 0.1$ – weight of degree difference (Δ_v)
$w_2 = 0.05$ – weight of sum of the distances between node v with all its neighbors (D_v)
$w_3 = 0.1$ – weight of mobility speed of every node (M_v)
$w_4 = 0.05$ – weight of cumulative time (T_v)
$w_5 = 0.3$ – weight of initial energy (E_v)
$w_6 = 0.4$ – weight of distance between Base Station to each sensor node (BS_v)

3.2 Energy Computational Model

The cluster head $\boldsymbol{CH}$ and base station $\boldsymbol{BS}$ both used some energy for the detection of collaborative black hole attacks. Using the first order radio model parameters [20], the energy consumed by an individual cluster head $\boldsymbol{CH}$ for receiving data packets $\boldsymbol{DP_s}$ from cluster members $\boldsymbol{CM_s}$ and transmitting them to base station $\boldsymbol{BS}$ and also for attack detection $\boldsymbol{E_{CHD}}$ is denoted by $\boldsymbol{E_{CH}}$, is formulated in $(\mathbf{2})$. The $\boldsymbol{E_{elec}, E_{amp}, and\ E_{DA}}$ are constants. The total energy consumed by all cluster heads $\boldsymbol{CH_s}$ using the same manner in the network is denoted by $\boldsymbol{E_{TOT\_CH}}$, is formulated in $(\mathbf{3})$. The energy consumed by an individual clustet member $\boldsymbol{CM}$ for transmitting data packets $\boldsymbol{DP_s}$ to cluster head $\boldsymbol{CH}$ which is in the range of data transmission $\boldsymbol{RTx^2}$, is formulated in $(\mathbf{4})$. The total energy consumed by all cluster members $\boldsymbol{CM_s}$, is formulated in $(\mathbf{5})$. The energy consumed by base station $\boldsymbol{BS}$ for receiving data packets $\boldsymbol{DP_s}$ from cluster heads $\boldsymbol{CH_s}$ and for attack detection $\boldsymbol{E_{BSD}}$, is formulated in $(\mathbf{6})$. The total energy consumed by whole network under the attack and detection of collaborative black holes, is formulated in $(\mathbf{7})$.

$$\mathrm{E_{CH}} = \left(\mathrm{E_{elec}} * \mathrm{k} * \mathrm{CH_{degree}} + \mathrm{E_{DA}} * \mathrm{k}\right) + \left(\mathrm{E_{elec}} * \mathrm{k} + \mathrm{E_{amp}} * \mathrm{dtonextCH}^2 * \mathrm{k}\right) + \mathrm{E_{CHD}} \tag{2}$$

where k = number of bits transmitted, CH_{degree} = degree of cluster head, $d_{tonextCH}$ = distanced between two cluster heads.

$$\mathrm{E_{TOT\_CH}} = \mathrm{E}_{CH_1} + \mathrm{E}_{CH_2} + \mathrm{E}_{CH_3} + \cdots + \mathrm{E}_{CH_{NC}} \tag{3}$$

where NC represents number of clusters.

$$\mathrm{E_{CM}} = \left(\mathrm{E_{elec}} * \mathrm{k}\right) + \left(\mathrm{E_{amp}} * \mathrm{RTx}^2 * \mathrm{k}\right) \tag{4}$$

$$\mathrm{E_{TOT\_CM}} = (\mathrm{N} - \mathrm{NC}) * \mathrm{E_{CM}} \tag{5}$$

where N represents number of nodes.

$$\mathrm{E_{BS}} = \left(\mathrm{E_{elec}} * \mathrm{k} + \mathrm{E_{amp}} * \mathrm{RTx}^2 * \mathrm{k} + \mathrm{E_{DA}} * \mathrm{k}\right) + \mathrm{E_{BSD}} \tag{6}$$

$$E_{TOT} = E_{TOT\_CH} + E_{TOT\_CM} + E_{BS} \tag{7}$$

3.3 Metrics Definitions

Energy Consumption: The total energy consumption level can be calculated by taking the difference between the current energy $\boldsymbol{E_c}$ level and initial energy $\boldsymbol{E_i}$ level for the entire network node's. The consumed amount of energy level can be computed as:

$$Energy\ Consumption = \sum_{k=0}^{n} E_c - E_i \tag{8}$$

Packet Delivery Ratio: The packet delivery ratio is measured by total number of packets received at destinations D_p divided by the total number of packets sent from the source S_p, is formulated in (9).

$$Packet\ Delivery\ Ratio = \sum_{p=1}^{n} \frac{D_p}{S_p} \times 100 \tag{9}$$

Average End to End Delay: All possible delays in the network are included in average end to end delay, i.e., retransmission delays at MAC, buffering route discovery latency and propagation and transmission delay. The formula of an average end to end delay is given below.

$$Average\ End\ to\ End\ Delay = \sum_{i=1}^{n} \frac{(T_{ri} - T_{si})}{n} \times 1000 \tag{10}$$

where T_{ri} is reception time, T_{si} is send time and n is the number of packets delivered successfully.

Average Throughput: An average throughput is the total throughput of the network which refers to the number of data packets successfully transferred from a source to a destination "$\sum ReceivedSize$" in a given time "$Stoptime - StartTime$" is calculated as follows:

$$Average\ Throughput = \left(\frac{\sum ReceivedSize}{StopTime - StartTime}\right) \times \frac{8}{1000} \tag{11}$$

4. Proposed Detection Model against Collaborative Black Hole Attacks

Due to Collaborative black hole attacks in the network packets delivery time to the destination gets affected and producing long delay and also decrements in a throughput. Here, we proposed a collaborative black hole attack detection model which detects the collaborative black hole attacker nodes and produce the safe route to the destination. The following steps are taking for our proposed model against collaborative black hole attacks.

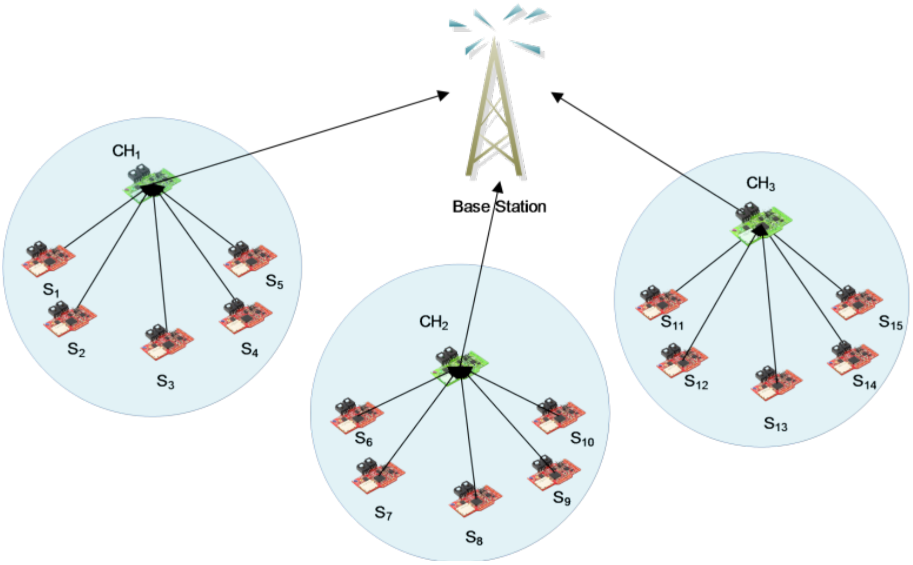

Fig. 1. Clusters without Collaborative Black Hole Attacks

Step1: We deployed the mobile nodes and a base station (BS) by using zigzag model in a rectangular field [21]. The base station is fixed and located within the mobile nodes.
Step2: The mobile nodes are randomly divided into clusters which are in the communication range of each other based on node distance using OWCA technique.

$$N(v) = \{v' | distance(v, v') \leq R_v\}$$

where $N(v)$ is the neighbor node, "v" is the every mobile node and R_v is the transmission radius.
Step3: The mobile nodes elect the cluster head node (CH) based on minimum weight and high energy as described in **Table 4**. OWCA is used for the election of cluster head.
Step4: The mobile nodes are randomly divided into different clusters. Each cluster has a cluster head while some cluster members are in communication range with cluster head based on node distance using OWCA technique. When a cluster is formed, it's the responsibility of cluster head to detect the malicious nodes in that cluster where the cluster head has the control on mobile nodes within the cluster. A table is maintained by cluster head via assigning $ID's$ and sequence numbers (Seqno) to all mobile nodes within the cluster as shown in **Table 2**. When all clusters are formed, it's the responsibility of base station to detect if any of the cluster head becomes the malicious node. The base station has the control on cluster heads. A table is maintained by base station via assigning $ID's$ and sequence numbers to all cluster heads within the network as shown in **Table 3**.

Table 2. Maintained by Cluster Head

Mobile Node	**ID**	**Seqno**
SN$_1$	IDS$_1$	2
SN$_2$	IDS$_2$	2
….	….	….
SN$_n$	IDS$_n$	2

Table 3. Maintained by Base Station

Cluster Head	**ID**	**Seqno**
CH_1	$IDCH_1$	3
CH_2	$IDCH_2$	3
….	**….**	**….**
CH_n	$IDCH_n$	3

Table 4. Electing Cluster Head

Algorithm 1

Input: m_selfWeight and m_Weight are the node weights, state = status of the **mobile** node
Output: Electing Cluster Head

```
ELECT-CLUSTER-HEAD( )
  RemovePositionTable( )                /*call function to remove the nodes position from the table*/
  UpdateNodePosition( )                 /*call function to update the new nodes position in the table*/
  neighborNodeList.clear( )             /*to clear neighbor nodes list of each node*/
  FindNeighborNodes(GetSelfNode( ))     /*get the new neighbor nodes of each node*/
  m_selfWeight ← GetNodeWeight(GetSelfNode( ))   /*get node weight*/
  for it ← neighborNodeList.begin() to neighborNodeList.end ( )
    m_Weight ← GetNodeWeight(GetSelfNode(*it))   /*get new node weight*/
      if m_Weight < m_selfWeight then            /*if new node weight is < previous node weight*/
          CH ← *it  /*elect cluster head (CH) based on minimum weight*/
          state ← SENSOR                         /*status of the mobile node*/
          m_selfWeight ← m_Weight                /*assign new node weight to previous weight*/
      end-if
  end-for
```

Step5: In base station authentication process, the base station sends an Authentication Packet (AP) to each of the cluster head in the sensor network. The authentication packet is shown in **Fig. 2** with authentication bit contains two values 0 and 1.

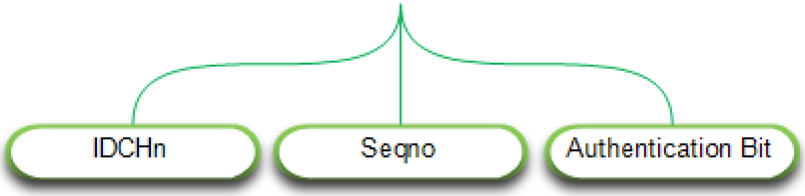

Fig. 2. Base Station sends Authentication Packet to CH_s

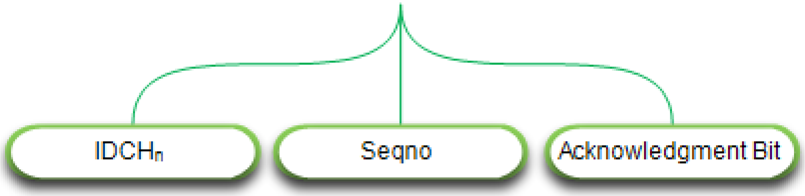

Fig. 3. Cluster Head's sends Acknowledgment Packet to BS

Fig. 3 shows the structure of the reply packet (RREP). Acknowledgment bit is used for an authentication purpose to prove that the reply is coming from authenticated node and acknowledgment bit contains two values 0 and 1.

In cluster head authentication process, Cluster head in the sensor network sends the Authentication Packet to each node in the cluster. This authentication packet contains three fields, ID of the node, sequence number and an authentication bit as shown in Fig. 4, which make it possible to recognize the authenticity of a mobile node. Authentication bit contains two values 0 and 1.

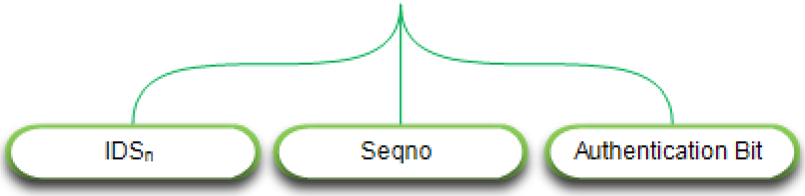

Fig. 4. Cluster Head sends Authentication Packet to CM$_s$

Fig. 5 shows the reply packet structure which contains three fields. The ID of the node, sequence number and acknowledgment bit field having a particular bit is set which obtained by increment one to the Authentication bit.

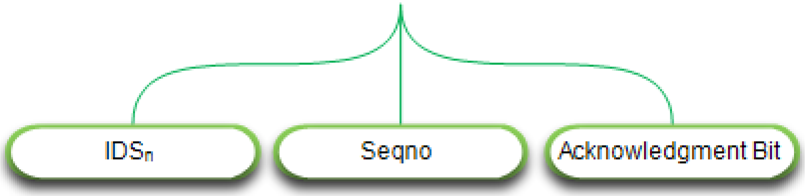

Fig. 5. Cluster Members sends Acknowledgment Packet to CH

Step 6: Fig. 1 shows the normal flow of traffic in a mobile ad hoc network. Mobile nodes $(S_1, S_2, \dots, S_{15})$ sense a physical phenomenon and converts this into information and pass that information to their respective cluster head in the form of data packets (DPS).

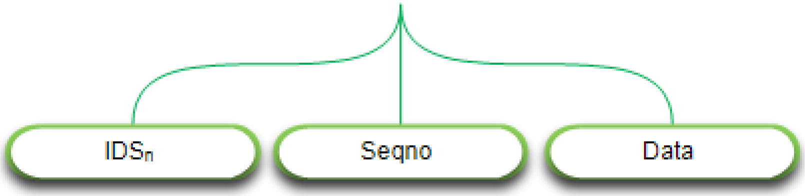

Fig. 6. Data Packet Fields

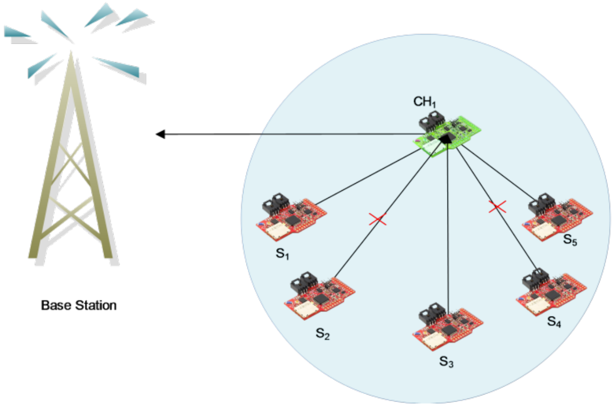

Fig. 7. Cluster with Collaborative Black Hole Attacks

Data packets (DPS) contain three fields, the ID of the source node, sequence number of the node who is sending the data packet as shown in Fig. 6. Collaborative black hole attacker nodes (S_2 and S_4) will not send any data packets to cluster head as shown in Fig. 7 Cluster head waits (wait-ch) for a fixed period of time. If the malicious nodes (S_2 and S_4) in the cluster do not send any packet even after this time period, which means the attacker nodes exist inside the cluster. The detection of collaborative black hole nodes occurs by cluster head through $ID's$ of IDS_2 and IDS_4, which are detected because they are sending the reply packets but not the data packets. Cluster head removes attacker nodes from their routing table and calls the procedure of electing cluster head for affected clusters after broadcasting in a network. Now by re clustering other nodes covered the area left unattended due to attacker nodes.

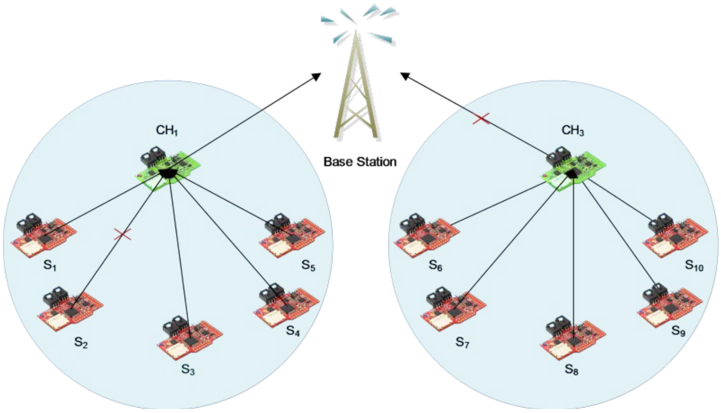

Fig. 8. Network with Collaborative Black Hole Attack

Cluster member and cluster head become collaborative black hole attacker nodes: Fig. 8 shows that the mobile node (S_2) and cluster head (CH_3) which collected data from all nodes in the cluster but does not send any data packets to cluster head and the base station respectively. Cluster head and base station waits for a fixed period of time. Even after this time period, if a mobile node (S_2) and cluster head (CH_3) does not send any packets, these nodes will detect as collaborative black hole attacker nodes. Cluster head and base station send a stop packet to the source nodes in a cluster, after getting a stop packet from cluster head and base station, source nodes stop sending data packets to both cluster head and the base station, after that remove the malicious nodes from their routing tables.

Table 5. **Detection and Prevention of CBHA**

Algorithm 2

Input: Initialization parameters, ch= cluster head, bs= base station, c= electing cluster head
Output: Detection of collaborative black hole attacks and removal of them from routing table

```
1. DETECT-PREVENT-ATTACKER( )
2.    Mobile nodes s= {$S_1$, $S_2$, $S_3$…, $S_n$} divided into clusters c= {$C_1$, $C_2$, $C_3$..., $C_m$} using (OWCA)
3.    $\forall\ C_i \in$ c $C_i$.ElectClusterHead( ), $m \geq i \geq 1$        /*$C_i$ is cluster head from each cluster*/
4.    $C_i$.sendAP()          /*cluster head send authentication packet to their cluster members*/
5.    bs.sendAP()             /*base station send authentication packet to cluster heads*/
6.    $C_i$.receiveRP( )      /*cluster head receive the response packet from cluster members*/
7.    bs.receiveRP( )         /*base station receive response packet from cluster heads*/
8.    if ResponsePacket = 1 and DataPacket = 1 then
9.        Goto step 4
10.   elseif ResponsePacket = 0 and DataPacket = 0
11.       NodeFailure( )
12.   elseif ResponsePacket = 1 and DataPacket = 0
13.       DetectionAndRemoveFromRoutingTable (*bh)    /*bh is black hole nodes*/
14.   end-if
15.   ElectClusterHead( )          /*Call the procedure of electing cluster head*/
```

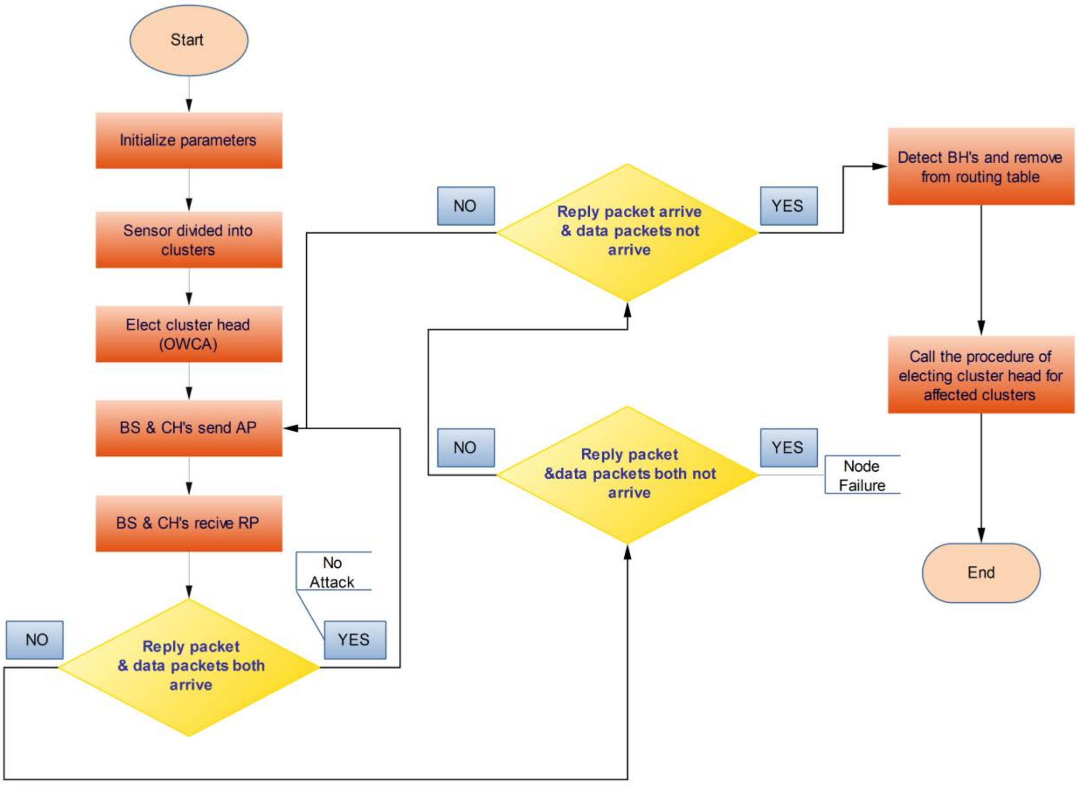
Start
Initialize parameters
Sensor divided into clusters
Elect cluster head (OWCA)
BS & CH's send AP
BS & CH's recive RP
NO
Reply packet & data packets both arrive
YES
No Attack
NO
Reply packet & data packets not arrive
YES
Detect BH's and remove from routing table
NO
Reply packet &data packets both not arrive
YES
Node Failure
Call the procedure of electing cluster head for affected clusters
End

Fig. 9. Proposed Design Flow

In **Fig. 8** a mobile node ($\boldsymbol{S_2}$) and cluster head ($\boldsymbol{CH_3}$) becomes the collaborative black hole nodes as they consume all the data packets coming from the mobile nodes without forwarding them to the cluster head and base station respectively. The cluster head and base station detects the collaborative black hole nodes through their $\boldsymbol{ID's}$ and remove malicious nodes from their routing table and call the procedure of electing cluster head for affected clusters after broadcasting in a sensor network as described in **Table 5**, because they were sending the reply packet but not the data packets as shown in **Fig. 9**. Now by re clustering of affected clusters the new cluster heads are selected based on minimum weight and high energy.

5. Simulation Results

5.1 Simulation Setup

Our detection model of collaborative black hole attacks performance is analyzed under the network simulator NS-2. The model of our experiment is built on 100 nodes distributed randomly with their unique identities on a network surface of $1500 \times 1000m^2$. To evaluate the efficiency of our protocol, we assume a mobile ad hoc network then 100 mobile nodes are initialized with 100 joules of energy.

Some of the network simulation parameters are used in our proposed experiment as driven from [22]. The network simulation parameters are mentioned below in the **Table 6**.

Table 6. Simulation Parameters

Parameter	Value
Number of Nodes	100 (mobile nodes)
Sink	1 static sink
Network Surface ($X \times Y$)	$1500 \times 1000m^2$
Transmission Range (r)	$250m$
Mobility Model	Random way point
Electronics Energy E_{elec} (Compute Energy)	$50nj/bit$
Amplifier Energy E_{amp} (Propagation Energy)	$100nJ/bit/m^2$
Aggregation Energy E_{DA}	$50nJ/\ bit/Signal$
Simulation Time	$300sec$
Traffic Type	CBR (Constant Bit Rate)
Packet Size	128 bytes
Number of Attacker Nodes	≥ 2
Propagation Model	Two-Ray Ground Model
Energy of Node	$100J$
Routing Protocol	AODV-OWCAS
Mobility	$50ms$
Weights ($w1, w2, w3, w4, w5, w6$)	$(0.1, 0.05, 0.1, 0.05, 0.3, 0.4)$

We assume that there are 8 collaborative black hole nodes randomly deployed in the network field. Those attacker nodes can be selected cluster member nodes or cluster head nodes as well.

The proposed OWCAS protocol which is the modified form of AODV with security is used to detect and prevent those collaborative black hole nodes from routing table to get the safe route to base station. The simulation results presented below as a comparison of DRIAODV Protocol under collaborative black hole attacks and EDRIAODV protocol under collaborative black hole attacks with our proposed OWCAS protocol under collaborative black hole attacks.

5.2 Evaluation and Results

To evaluate the performance of DRIAODV, EDRIAODV and OWCAS under collaborative black hole attacks, the following performance metrics are given.

To improve the network performance, we proposed a methodology where results are much better and acceptable under this scenario. It offers a great deal of improved results as compared to the existing techniques as well as it is much energy efficient. Performance of Ad hoc on-Demand Distance Vector protocol under collaborative black hole attack is measured in terms of throughput, average end-to-end delay, average energy consumption, and packet delivery ratio. The improved results of various performance metrics are shown in a graphical view **Fig. 10-13**.

5.2.1 Energy Consumption

In this subsection, the impact of the number of nodes on the performance of the OWCAS with and without energy computational model, is evaluated. In the previous existing schemes none of them have focused on energy consumption under collaborative black hole attack. In this simulation the energy consumption is measured as the number of nodes increased to 100.

Fig. 10 presents the energy consumption as number of nodes varies. This figure demonstrates that, with energy computational model the proposed OWCAS protocol consumed less energy as compared to without energy computational model in OWCAS.

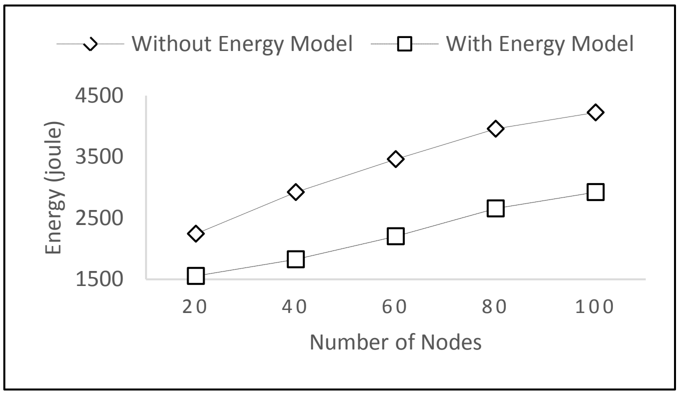

Fig. 10. Energy Comparison With and Without Energy Model

5.2.2 Packet Delivery Ratio

Fig. 11 shows the comparison of a packet delivery ratio over number of nodes between DRIAODV, EDRIAODV and OWCAS. From the graphical presentation of a packet delivery ratio shows much better results in case of OWCAS as compared to DRIAODV and EDRIAODV. As the number of nodes increases, the packet drop increases which results in a decrement of a packet delivery ratio. When the collaborative black hole attacking nodes remove from the routing table, data packets delivered to the destination successfully and it will increase the packet delivery ratio.

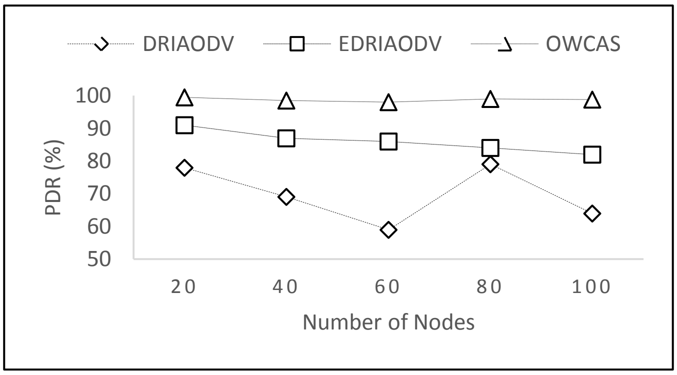

Fig. 11. PDR Comparison of DRIAODV, EDRIAODV and OWCAS

5.2.3 Average End to End Delay

Fig. 12 shows the comparison of end to end delay between DRIAODV, EDRIAODV and OWCAS varying with number of nodes. Due to collaborative black hole attacks, a data packet does not reach the destination on time which produces long delay in the network. When collaborative black hole attacker nodes are removed from the routing table, then the data packets are sent to the destination nodes successfully on time, our proposed protocol has much better result as compared to the existing schemes.

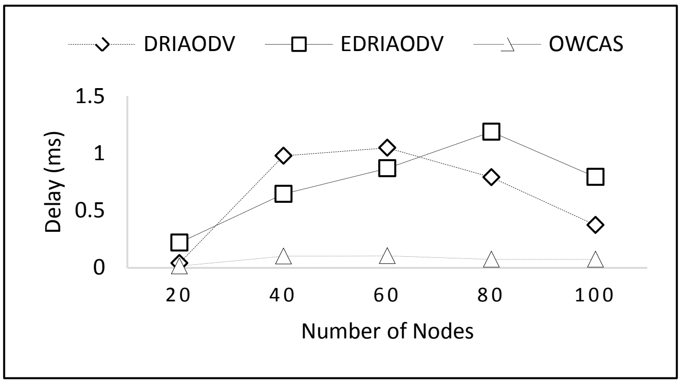

Fig. 12. Delay Comparison of DRIAODV, EDRIAODV and OWCAS

5.2.4 Average Throughput

Fig. 13 shows the comparison of throughput between DRIAODV, EDRIAODV and OWCAS. The comparison in graph shows that the throughput over number of nodes is better in the case of OWCAS as compared to the existing schemes.

AODV routing protocol does not have any security mechanism due to the fact that collaborative black hole nodes drop the data packets in the network and also decreases the throughput of the network. As the number of mobile nodes increases the data packets drop increases, which results in a decrement in the throughput. In our proposed model, when collaborative black hole attacking nodes removed from the routing table, the data packets are sent to the destination successfully and a throughput of the network increased.

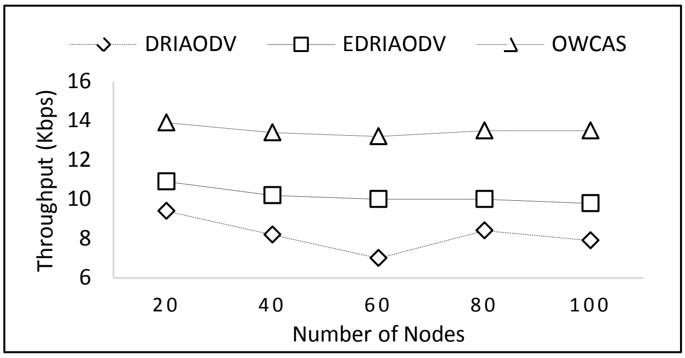

Fig. 13. Throughput Comparison of DRIAODV, EDRIAODV and OWCAS

6. Conclusion

A deep and detailed study of the collaborative black hole attacks in a mobile ad hoc network gives a great deal of improved solution to diminish collaborative black hole attacks. The proposed scheme comes up with enhanced results as compared to earlier methodologies with much energy efficient. Currently, one of the key concerns in network design is energy efficiency and unfortunately much attention was not paid in the previous approaches. While implementing our scheme, we consider sensors' energy as a key feature with a better packet delivery ratio, lower delay time and high throughput which shows an improved performance and high benchmark results. This paper has shown that throughput and packet delivery ratio increases while the end to end delay decreases as compared to existing schemes. It also reduces the overall energy consumption and network traffic by maintaining accuracy and high detection rate. The research work will be extended in future in terms of performance metrics and comparing this proposed scheme with other clustering methodologies and protocols to obtain further better results.

Acknowledgment

The authors would like to thank the anonymous reviewers for the helpful comments and suggestions. The authors are also grateful to Fundamental Research Funds for the Central Universities NO. WK2150110007 and National Natural Science Foundation of China (Grant No. 61772490, 61472382, 61472381 and 61572454) for its financial supports.

Conflict of Interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

Disclosure

Muhammad Umar Farooq and Xingfu Wang are the first authors.

References

[1] S. Dixit, T. Ojanpera, R. van Nee, and R. Prasad, "Introduction to globalization of mobile and wireless communications: today and in 2020," *Globalization of Mobile and Wireless Communications, Springer Netherlands*, pp. 1-8, 2011. Article (CrossRef Link).

[2] K. Xing, S. S. R. Srinivasan, M. Rivera, J. Li and X. Cheng, "Attacks and countermeasures in sensor networks: A survey," *in Network Security*, Springer US, pp. 251-272, 2010. Article (CrossRef Link).

[3] D. Sheela, V. R. Srividhya, A. Begam, Anjali and G. M. Chidanand, "Detecting black hole attack in wireless sensor network using mobile agent," in *Proc. of Int. Conference on Artificial Intelligence and Embedded Systems*, pp. 45-48, 2012.

[4] J. Kaur and B. Kaur, "BHDP using fuzzy logic algorithm for wireless sensor network under black hole attack," *International Journal of Advance Research in Computer Science and Management Studies*, pp. 142-151, 2014.

[5] D. Sheela, C. N. Kumar and G. Mahadevan, "A non-cryptographic method of sink hole attack detection in wireless sensor networks," in *Proc. of Int. Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 527-532, 2011. Article (CrossRef Link).

[6] F. J. Zhang, L. D. Zhai, J. C. Yang and X. Cui, "Sinkhole attack detection based on redundancy mechanism in wireless Sensor Networks," in *Proc. of 2nd Int. Conference on Information Technology and Quantitative Management*, ITQM, pp.711-720, 2014. Article (CrossRef Link).

[7] V. K. Verma, S. Singh and N. P. Pathak, "Analysis of scalability for AODV routing protocol in wireless sensor networks," *International Journal for Light and Electron Optics*, pp. 748–750, 2014. Article (CrossRef Link).

[8] M. U. Farooq, X. Wang, R. Yasrab and S. Qaisar, "Energy Preserving Detection Model for Collaborative Black Hole Attacks in Wireless Sensor Networks," in *Proc. of IEEE 12th Int. Conference on Mobile Ad-Hoc and Sensor Networks*, pp. 395-399, 2016. Article (CrossRef Link).

[9] H. Weerasinghe, and Fu. Huirong, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. of IEEE Future generation communication and networking*, pp. 362-367, 2007. Article (CrossRef Link).

[10] M. N. Sharma and M. A. Sharma, "The black-hole nodes attack in MANET," in *Proc. of 2nd International Conference on Advance Computing and Communication Technologies*, pp. 546-550, 2012. Article (CrossRef Link).

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya and K. E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc network," in *Proc. of Intl. Conference on Wireless Networks*, pp. 570-575, 2003.

[12] F. Shi, W. Liu, D. Jin and J. Song., "A cluster-based countermeasure against black hole attacks in MANET," *Telecommunication Systems*, pp. 119-136, 2014. Article (CrossRef Link).

[13] F. H. Tseng, L. D. Chou and H. C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Computing and Information Sciences*, 2011. Article (CrossRef Link).

[14] M. Wazid, A. Katal, R. S. Sachan and R. H. Goudar, "Detection and prevention mechanism for black hole attack in wireless sensor network," in *Proc. of IEEE Int. Conference on Communication and Signal Processing*, pp. 576 – 581, 2013. Article (CrossRef Link).

[15] G. S. Bindra, A. Kapoor, A. Narang and A. Agrawal "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," in *Proc. of IEEE Int. Conference on System Engineering and Technology (ICSET)*, pp. 1-5, 2012. Article (CrossRef Link).

[16] V. A. Hiremani and M. M. Jadhao, "Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET," in *Proc. of IEEE Int. Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, pp. 944-948, 2013. Article (CrossRef Link).

[17] G. Wahane and S. Lonare, "Technique for detection of cooperative black hole attack in MANET," in *Proc. of IEEE 4th Int. Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1-8, 2013. Article (CrossRef Link).

[18] S. Biswas, N. Tanumoy and N. Sarmistha, “Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET,” in *Proc. of IEEE Conference on Applications and Innovations in Mobile Computing (AIMoC)*, pp. 157-164, 2014. Article (CrossRef Link).

[19] N. V. Babu, S. B. Boregowda, C. Puttamadappa and S. D. Shivaraj, “An optimized weight based clustering algorithm in heterogeneous wireless sensor networks,” *Computer Science & Information Technology*, pp. 185-195, 2012.

[20] A. Hawbani, X. Wang, H. Kuhlani, S. Karmoshi, R. Ghoul, Y. Sharabi and E. Tarbosh, “Sinkoriented tree based data dissemination protocol for mobile sinks wireless sensor networks,” *Wireless Networks*, pp. 1-12, 2017. Article (CrossRef Link).

[21] A. Hawbani, X. Wang, S. Karmoshi, L. Wang and N. Husaini, “Sensors Grouping Hierarchy Structure for Wireless Sensor Network,” *International Journal of Distributed Sensor Networks*, pp. 1-18, 2015. Article (CrossRef Link).

[22] S. Mahajana, J. Malhotrab and S. Sharma, “An energy balanced QoS based cluster head selection strategy for WSN,” *Egyptian Informatics Journal*, pp. 189-199, 2014. Article (CrossRef Link).

[23] G. Wahane, A.M. Kanthe, and D. Simunic, “Technique for detection of cooperative black hole attack using true-link in Mobile Ad-hoc Networks,” in *Proc. of IEEE 37th Int. Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1428-1434, 2014. Article (CrossRef Link).

[24] S. Malik and I. Kashyap, “Identifying, Avoidance and Performance Assessment of Black Hole Attack on AODV Protocol in MANET,” *International Journal of Computer Applications*, pp. 6-11, 2014. Article (CrossRef Link)

[25] A. Siddiqua, K. Sridevi and A. A. K Mohammed, “Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm,” in *Proc. of IEEE Int. Conference on Signal Processing and Communication Engineering Systems (SPACES)*, pp. 421-425, 2015. Article (CrossRef Link).

Muhammad Umar Farooq received his B.S. degree from International Islamic University Islamabad, Pakistan in 2012 and received his M.S. degree in Computer Science and Technology from University of Science and Technology of China in July 2017. He is doing Ph.D. in Computer Science and Technology from University of Science and Technology of China. His main research interests include WSN, Network Security and IoT.

Xingfu Wang received the B.S. degree in electronic and information engineering from Beijing Normal University of China in 1988, and the M.S. degree in computer science from the University of Science and Technology of China in 1997. He is an associate professor in the School of Compute Science and Technology, University of Science and Technology of China. His current research interests include Information Security, Data Management and WSN.

Moizza Sajjad received her BSc. degree from Gomal University, Pakistan. Currently she is a student of Master degree program. Her main research interests include WSN and Cloud Computing.

Sara Qaisar received her BSc degree from Punjab University, Pakistan in 2008, MBA degree in Information Technology Management and M.S. degree in Technonology Management from International Islamic University Islamabad, Pakistan in 2012 and 2016 respectively. She is doing Ph.D. in Science and Technology Communication and Policy from University of Science and Technology of China. Her main research interests include Diffusion of Innovation, Cloud Computing Securtiy, Technology and Business Incubation, Network Security and WSN.