Detection and Prevention of Black Hole Attacks in IOT & WSN

Shoukat Ali[1], Dr. Muazzam A Khan[1], Jawad Ahmad[2], Asad W. Malik[1], and Anis ur Rehman[1]
[1]Department of Computing, SEECS, National University of Sciences and Technology, Islamabad, Pakistan.
[2]Glasgow Caledonian University, School of Engineering and Built Environment, Glasgow, UK.
Sali.msis16seecs@seecs.edu.pk, Muazzam.khattak@seecs.edu.pk.

Abstract — **Wireless Sensor Network is the combination of small devices called sensor nodes, gateways and software. These nodes use wireless medium for transmission and are capable to sense and transmit the data to other nodes. Generally, WSN composed of two types of nodes i.e. generic nodes and gateway nodes. Generic nodes having the ability to sense while gateway nodes are used to route that information. IoT now extended to IoET (internet of Everything) to cover all electronics exist around, like a body sensor networks, VANET's, smart grid stations, smartphone, PDA's, autonomous cars, refrigerators and smart toasters that can communicate and share information using existing network technologies. The sensor nodes in WSN have very limited transmission range as well as limited processing speed, storage capacities and low battery power. Despite a wide range of applications using WSN, its resource constrained nature given birth to a number severe security attacks e.g. Selective Forwarding attack, Jamming–attack, Sinkhole attack, Wormhole attack, Sybil attack, hello Flood attacks, Grey Hole, and the most dangerous BlackHole Attacks. Attackers can easily exploit these vulnerabilities to compromise the WSN network.**

Keywords: ***WSN, Security, Generic Nodes, Gateway Nodes, Sensor, Vulnerabilities, Attacks, Black Hole***

I. INTRODUCTION

WSN is a network of low cost and small sensing devices called sensors. Sensor nodes possess a unique identity with the capability to sense, process and share the data with other devices. WSN are not only limited to the components of small sensing devices e.g. a temperature sensing device to the most critical and complex parts of a jet-engine. Smart home appliances like air conditioners adjusting room temperatures by sensing your body's temperature. Motion detecting devices alert you about a suspicious activity. WSN nodes are less expensive and easy to deploy, using wireless medium for communication. Sensor nodes are limited in battery power, processing and computations. These devices cannot be protected using conventional cryptographic algorithms. Resource constrained nature and using wireless medium make them vulnerable to many attacks. Black hole attack is one of them. Hackers can easily penetrate into the network and compromise these nodes. A comprehensive research has been done so far, but still more efficient work will be required to prevent sensor networks from such attacks.

WSN is a network of self-organized and less expensive devices. These devices use sensors and actuators thus minimizing human interaction. WSN devices can be used for a specific or variety of purposes e:g military, homes, health care industry [1][2]. A thing in IoT can be a human, a health care monitoring device, a smartphone, smart grid Stations, autonomous cars , smart watches, body sensing devices and smart home appliances. These devices use wireless connections to share information [2][3]. WSN consists of small devices, installed in different areas where human access may not be possible. These nodes are called sensor nodes. Sensor node can collect, process and transmit the data to the base stations. These nodes convert environmental information like temperature, humidity and air into electrical signals. WSN can be used for different purposes, most important applications are military, control, tracking, homes industry, space, pollution observation, environmental / earth sensing, forest fire detection, landslide detection, knowledge work, health care and Smart Grids [4][3].

WSN use wireless medium for transmission. Data transmission over wireless medium is cost effective and minimize the human effort to place cables over large geographic areas [6]. WSN devices are working together to collect and exchange data for different kind of purposes. Sensor nodes not only used in normal environmental conditions but also in critical infrastructures [7]. MANET's (mobile adhoc networks) composed of mobile nodes with limited transmission range, battery and processing power [8]. Sensor nodes are very economical and deployed in areas where human approach is not possible. WSN nodes are capable to sense the environmental conditions and forward it [11]. Hierarchical structure based WSN consists of base Station, cluster heads and member nodes. CH receive the data from member nodes and send that information to the base station. Figure 1 shows the operation of a cluster based WSN [12]. Mobile adhoc network (MANET) consist of nodes that can freely join or leave the network. There is no specific structure for MANET nodes. Self-organizing nature of these nodes made them popular candidate for military and disaster management application [14]. WSN is a combination of nodes that are connected together to communicate [17].

WSN devices spread over large geographic areas. Due to its open nature and wireless connectivity, these networks are vulnerable to different kind of attacks. Some well-known attacks are Jamming, Wormhole, Sinkhole, Sybil, Selective Forwarding, hello Flood, Grey Hole and Black Holes. Black hole (BH) considered as one of the most dangerous and an entry point for all other attacks [1] [2]. Nodes compromised by a BH

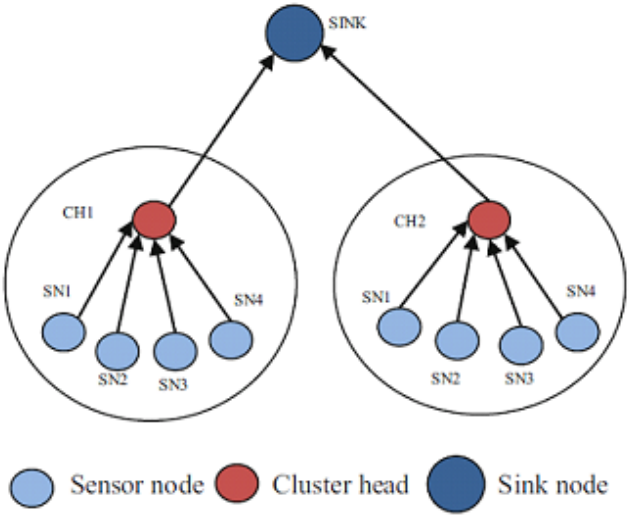

Figure 1: Cluster based WSN [12]

attack are called malicious nodes. In a BH attack the bad nodes advertise the wrong path to the network that it has the freshest and small route to the destination. The intensions of these bad nodes are to attract more traffic and then start dropping those packets instead of forwarding [2]. BH attack is basically a DOS attack for the degradation of network performance. During the BH attack, the node blocks / drops incoming data instead of sending towards the receiver [4]. Black hole is the malicious behaviour of a node claiming that it has the smallest path towards the destination. The purpose of a Black Hole attack is to drop the incoming data packets [5]. WSN use radio frequencies for sending and receiving data over wireless networks. There lies different problems leading to many attacks, Denial of service is one of them [6]. The limited resources of WSN devices make them vulnerable to many security threats. BH attack is one them. BH is basically a DoS attack, where an evil node advertise the smallest fake route to the destination. Malicious node absorbs all the traffic instead of forwarding [7][8].

The nodes in WSN environment depends on other nodes for data forwarding. The intruders use this hop-by-hop dependency and insert a bad node into the path. The bad node start dropping packets and hence a black hole attack occurs [9]. WSN nodes are limited in transmission, computation and power. Due to these limitations, traditional cryptographic solutions cannot be implemented in WSN that makes them vulnerable to many security attacks [10]. In a black hole attack, sink node is unable to receive enough data packets from a CH. BH attack can be further categorized into single and collaborative BH attacks. Single BH attack consists of only one malicious node while there are more than one malicious nodes in collaborative BH attack. Collaborative black hole attacks greatly affecting the network performance and are difficult to detect [11]. When a node absorb all the packets instead of forwarding, that node is called a black hole. Black hole attack greatly decrease the network throughput and the node's energy [12]. Black hole attack is basically a DOS attack because the node did not forward any or very little data packets. In this attack, a malicious node try to attract more traffic towards itself and then start dropping these packets instead of forwarding [14]

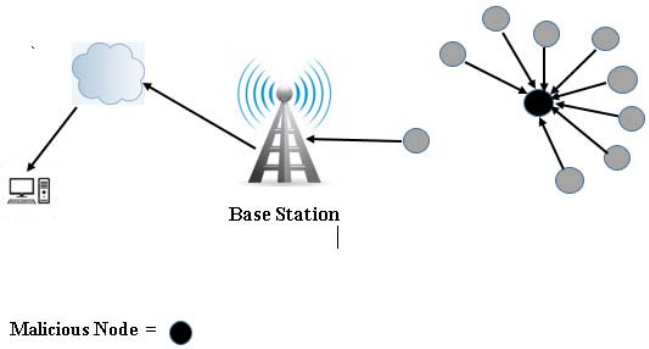

Figure 2: Black-Hole Attack [7]

Figure *2* shows that a node willing to transmit the sensed date to the base station (sink node). Sender broadcast RREQ (route request) packet to the network. Adjacent nodes will reply with RREP packet (route reply) if they have a freshest and smallest route to the target node.

The first node that reply before others will be selected for routing and transmission will be started. If a node doesn't have any path towards the destination, RREQ packet will be advertised further. Using the feature of RREP packet, the selfish nodes will reply for claiming the best path to reach the destination. Selfish nodes should reply first before other nodes, otherwise the attack will not work. The source node will start sending data packets towards the BH node. The compromised / bad node will start dropping the packets instead of forwarding. This will significantly increase end-to-end delay and will drain out node's energy more quickly. Packet delivery ratio and throughput will also be greatly affected.

Rest of the paper consists of the following sections; In section II, more recent Related Work is highlighted. We have discussed different techniques proposed for detection and prevention of BH attacks in detail. In section III various schemes have been compared with each other. Core strengths and weakness of each scheme is represented in the Table *1*. In Section IV, conclusion summarize the paper while in future work we recommend that new solutions will be required to efficiently dealt with black hole attacks.

II. RELATED WORK

WSN nodes are open to different security threats, Black hole (BH) attack is one of them. Different schemes are available to cope with the BH attacks. Shreenath K N et al. [1] presented the approach of Zoning method. WSN divided into different zones of the same size. Every zone assigned a unique ID. Localization algorithm applied so that every sensor node should know its location. All nodes share their energy levels with each other and base station. BS selects a node with highest energy as the head of that zone. CH is responsible to receive the data from its member nodes and send it to the base station. Mobile agents used to monitor each node and zone heads. If a node or the zone head unable to sent or receive data, mobile agent will mark that node as a

BH. Agent will alert the Zone head and Base Station to remove the malicious node from the network. Abhinav Kaurav et al. [2] proposed his idea to detect and prevent malicious nodes using network simulator 2.35. Tool command language (TCL) used to monitor the whole activity in the network. TCL generates three different files called terminal files, NAM (network animator) and Trace file. Terminal file shows the status and path followed by the packet. NAM is the visual representation of the packets flow (Simulation of the network). Trace file shows the details of the delivered or lost packets in the network. In the proposed scheme, a simple network consists of different nodes. A malicious node injected into network, to attract the maximum traffic by advertising a wrong path. For real time monitoring. Intrusion detection system installed on every node to observe its behaviour. Every node has a unique ID. If a node failed to forward the received data packets. IDS will mark the node as a malicious node and alert the base station. BS will remove the suspicious node from the network. Pavan Kumar et al. [3] presented the active detection protocols scheme to detect the malicious routes. Active detection routing protocol used to detect the intruder. Routing protocols attract the attacker to attack the path, when data packets are not there. Such suspicious paths will lose their trust and should be avoided in future. Similarly the trust of successful route will be incremented. Nodes with high trust and near to the sink will be used for data transmission. If there is no node near the sink, it will report back to higher node that destination is not reachable. The node will select another node with high trust for routing information.

In paper [4] HTB – BHD scheme has been proposed for Smart Grid stations. The Network is divided into different segments, and from each segment a CH is selected. Cluster head will be elected on weighted cluster head selection algorithm. CH collect the data and sent towards the Sink. Data aggregation model used to avoid duplicity, extra energy consumption and overhead issues. Hierarchical trust evaluation model implemented to differentiate good nodes from bad ones. The trust evaluation model can help the cluster head to determine the legitimacy of a node. Cluster head is responsible for maintaining the history of its own dropped packets. If the ratio of dropped packets is greater than the threshold, re-clustering will occur.

In [5] Anshuman Chhabra et al. presented a security mechanism based on game theory model and potential threat messages. In a game theory model, two players are trying to play the game for their own interest. In the propose model good and bad nodes play the game but with different intentions. The concept of Potential Threats (PT) messages used to detect the malicious nodes. PT messages basically help the nodes to decide whether to make contact with a particular node or not. In the beginning an average delay time (Threshold) for normal nodes are calculated. In the first step the time taken by a node for relaying a message has been noted. If the time is greater than the threshold, PT messages will be flooded into the network. Second the node involvement is being observed in the message and potential threats associated with those ID's. If the difference of relaying message and potential threats against it is greater than the threshold value, a connection will be established with the source node otherwise the request will be refused. Another option of game theory used to enable the normal node to co-operate or refuse the connection with a node. In this strategy the normal and attacker node adopt same strategies except the attacker attacks and normal node defend.

In [6] P. Hemalatha et al. using the concept of artificial Bee colony algorithm for detecting DoS attack. Honey Bee algorithm consist of Scouts, Onlookers and Employed Bees. Scouts are accountable for searching fresh food sources. Onlookers have the authority to make decision whether to select the food source or not. Employed Bees are Visiting the food source to take the food. In the proposed system the Artificial Bee Colony Algorithm is used along with Reverse Tracing Technique. Nodes will send the data through their neighbour. RREQ packet will be sending to the neighbour node. If the node replied, data transmission will be started otherwise mark that node as a black hole. Sender will check the next node for transmission.

In [7] Abdullah Aljumah et al. detecting the black hole attack using validation and response packets. The network consists of clusters and each cluster consists of a cluster coordinator and sensor nodes. A node with higher efficiency will be selected as the head called cluster coordinator (CC). CC is responsible to detect malicious nodes and store the ID's of all immediate and intermediate nodes. CC sends validation packet to the network indicating the ID of the immediate nodes. An additional bit sent along with the packet so the nodes can identify it as a validation-packet. Other nodes will send the response packet to acknowledge the receipt of validation packet. Response packet composed of immediate node ID and ACK field. CC collects the data from sensor nodes through immediate nodes. If the CC did not receive any packet from the immediate node within due time (packet arrival time), immediate node will be marked as black hole and thus removed from the network. Re-Clustering will occur and the nodes of malicious router will start sending information to the second router.

Saurabh Sharma et al. [8] proposed trust and reputation based scheme called CRCMD&R. Malicious nodes can be detected during route path setup. Hence the information should not be sent through these bad nodes / routes. The mechanism of CRCMD&R is almost same as AODV with some additional features. Cluster Head (CH) is responsible for maintaining three tables called neighbour's table, LVT (legitimacy value table) and RVT (Reputation level table). Neighbour's table contain the ID's of neighbouring nodes along with its CH ID's. Legitimacy value table is being used to keep the history for different nodes. How many times a node involved in a communication process, the ratio of successful to the total packets transmitted. This is helpful for calculating the fair (legitimate) value of a node. The node honesty or dishonesty can be predicted by using legitimacy value table. Another table named as reputation value table (RVT) is also maintained by the CH. RVT basically store reputation of a

node. Additional field of CH-ID added to the RREQ packet. This field stores the CH-ID of the source node. Similarly the RREP packet is also modified to store additional values. RREP field store Route Reply, consisting of;

- N_{RREP} ID: Node ID (node that replies)
- N_{RREP} next node: Node ID, Next to the replying node
- PPN of all nodes from source to destination (Each node has unique ID broadcasted)
- CH ID of N_{RREP} (replying node)

In RVT the reputation of a node must be higher than the threshold value. Only higher value nodes will be selecting for routing the packets. In the process of secure route discovery, sender will broadcast the RREQ packet to the network. The neighbour nodes will reply with RREP along with his ID, prime product of all nodes and CH ID. The source will divide the prime product on total number of nodes from source to destination. If the received prime product number is divisible by number of nodes in the path, that node will be marked as partially trusted. Source node will send dummy packets that node. If the N_{RREP} node lies within the same CH, CH enters in to the promiscuous mode and calculate the RV (reputation value) for the node. If the Source and replying node does not lie in the same Cluster, the CH of originator send encrypted information to the CH of IN (intermediate node). This information must be sent via reliable path. CH of IN enters into the promiscuous mode, calculate LV (legitimacy value) for IN, Next node and call the algorithms for detecting and removing co-operative BH nodes.

In [10] Mert Melih OZCELIK et al. proposed the methodology of Hybrid Trust Based Intrusion Detection System. All nodes and CH's will be managed by Base station. BS assign identities, sharing keys and initialize trust values. The sensor network is divided into three levels sensor, clusters and base station. Control Packets (CP) exchanged between the base station, CH and sensor nodes. CP's help the base station to select a CH if the current CH is not capable enough to handle queries. If a sensor node finds that its CH is malicious, the sensor will send control packet directly to the base station via alternate route. CP includes CH-ID, node ID's and consolidated trust values of Members. In case a sensor node is sending information directly then CP contains ID of its CH and trust value of CH. Every node is calculating the reputation value of CH and one hop neighbors. Reputation values stored in Function Reputation table (FRT) and then broadcasting the table into the network. The sensor node will monitor their neighbor nodes and calculating their FRT's. FRT values depends on reply of the nodes, a node's sensed data, response as per threshold, reliability of event reporting and forwarding of data. Data forwarding feature used by sensor nodes for CH. CH sending CP to the BS before sending information. Sensor must listen to those CP's and check for their ID's. If a node find that it's ID is not included in the CP, the node should increment Fail count for the CH otherwise Success count will be incremented. All nodes including Base Station maintain two tables, its own FRT and the FRT's received from other nodes. Consolidated trusted values calculated by comparing these two tables. The sensor can directly sent messages to the base station, if they found a particular CH is malicious by encrypting the CH ID. BS will decrypt the message received from sensor node, checking CH ID, hence isolate that specific CH from further communication.

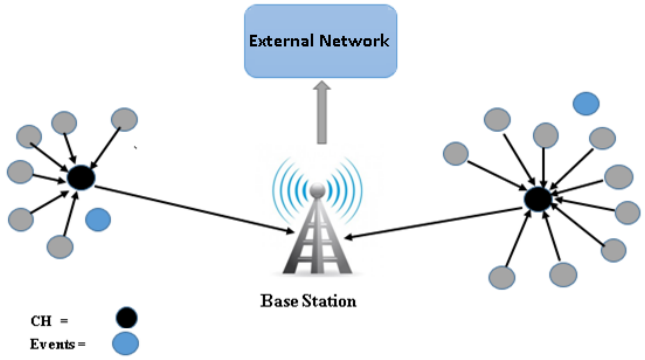

Figure 3: Hybrid Trust Based IDS for WSN [10]

Arshdeep Kaur et al. [11] presented a technique called hybrid trust based IDS for detecting BH attacks in WSN. HTB technique identify the attacks with the help of Received Packet and Time delay. The source node will send the RREQ to the network and wait for a specific amount of time (Threshold). For successful communication, nodes should reply before the threshold expires. Otherwise the node will be marked as a black hole. Source node will alert the network to avoid communication with the malicious node. Gurjinder Kaur et al. [12] discussed the mechanism to protect WSN from BH attacks. CH is the ideal point for an attacker to compromise. If the CH got compromised, maximum damage can be done to the network. The approach [12] focused on detecting and preventing a black hole attack in clustered base WSN. LEACH protocol is used in the proposed scheme to select the CH. CH is elected based on node energy and distance of the node from BS. If the energy of two nodes remain the same, node with optimal distance from BS will be selected as CH. CH selection process repeated again after a specific amount of time. BS will maintain and monitor the energy levels of already selected CH's. If the selected CH advertised same energy or a very low decrease in energy, will be considered as malicious. BS will alert the network about the suspicious node.

Moutushi Singh et al. [13] proposed the scheme of Two-Tier trust management to detect the malicious nodes in WSN. Communication and data trust are used to predict the reputation of neighbor nodes. CH will assign keys to the registered nodes. After successful registration, nodes can participate in communication. Old nodes can only take new keys when their trust value is higher than the threshold. Trust values will help in isolating bad nodes from the good ones. The nodes that are not participating in the communication process will lose their trust level, hence deleted from the network. In the second phase, CH start monitoring the whole network. The source nodes communicate with neighbor nodes by request-reply or Rcv – Ack signal. Only good nodes can follow this scheme, bad nodes may not follow this scheme. Legitimate node can request for data from their

neighbor nodes and after receiving the data they also send back Ack signal. Trust values incremented and decremented based on traffic. The nodes having trust value above or equal to threshold can be assigned a new key while those having less value will be gradually deleted from the network.

Ali Dorri [14] proposed a comprehensive methodology of EDRI (Extended data routing information). By using this technique cooperative BH attack can be detected and prevented in MANET's. EDRI approach is basically an extension to the DRI (data routing information) approach. EDRI table store neighbor node ID's, source node, To destination and Black hole node. ID field store the neighbor's ID, from (refers to source node), To field (refers to destination) and BHN refers to the black hole nodes. Two values 0 and 1 for each node will be used to indicate current state. If a bad node is detected, the value in BHN column will be changed to 1. Every node should maintain their own EDRI table. Control packets (CP) also used along with EDRI approach. CP consists of source node ID, its next node and random for security. The random number will remain the same throughout the data path. Data control packet cannot be forwarded by the malicious nodes so it can detect malicious node but fail in case of cooperative BH attacks. The propose scheme work in three different phases i:e finding the path, checking the path and eliminating the detected malicious nodes. For finding the freshest route the RREQ is broadcasted. The node responded with RREP will also sent their NHN and EDRI list. Malicious node will send their cooperative black hole ID in NHN to avoid detection. In the next step If this is the trusted path so the source will start sending packets otherwise the path is checked by using the proposed approach. Source node will generate a random number and setting itself to intermediate node (IN). Source will send the data control packet to NHN and wait for reply. If the random number received is same as sent, source (IN) should update its EDRI entries (from and through set to 1 for its next node). If the replied node is the last node, stop checking and end. If the received random number is different, mark the node as malicious and inform source node. If the NHN is not the last node then select NHN next node and mark as IN. Find a route to IN and ask for IN's next hope node and EDRI entries. Compare EDRI entries of IN with its previous node. If the From and To column of IN is set to 1 for its previous node, then the node is reliable otherwise malicious. If malicious then inform the network. Repeat the process till successful completion of packet. Every node is sending the data packet to its source and next node and also checking the replies of its NHN. If same, mark as trustable otherwise malicious. After detecting the malicious nodes, the source node will alert the network about the malicious node's ID. Nodes upon receiving the packet will set their BHN column to 1 against the BH-ID. Sensors will isolate the malicious node for further communication.

G. Arulkumaran, et al. [15] proposed the methodology of Fuzzy logic for detecting BH attacks. Fuzzy logic rule is used for trust management between two nodes. Each node is responsible to maintain the trust value of its neighbor nodes. Before communication, source node first compute the trust value for the route, and update that value in each node's routing table. The most reliable node is being selected for transmission. Neighboring node supports three different modes i:e like to forward, forwarding and source list. Forwarding list keep the record of packets that are already sent. Source nodes information will be stored in source list. Neighbor nodes are monitoring each other and increment or decrement their trust values. If a neighbor node forward the received packets, its trust will be increased. It is pretty much clear that nodes consume energy when they receive and forward data packets. As compared to normal nodes, malicious nodes consume less energy. Malicious nodes only receive packets and discard them. Energy supervisor is responsible for monitoring the energy level of all nodes in MANET environment. Direct and indirect trust mechanism used to confirm the trustworthiness of each node. Direct trust is the observation of a node about another node, while indirect trust is the observation of other nodes about a node. For nodes integrity packet veracity check is used. Digital signatures used with RSA to ensure integrity. Final trust values are calculated on the destination node. Destination node combine the trust values of nodes and compute the final trust value. A certificate authority is responsible for assigning certificates to high trust nodes. Only authorized nodes can take part in communication process. The legitimate or suspicious nodes will be identified by the CA. CA take decisions based on Fuzzy Analyzer algorithm, which is automatically called. In case a node is no more trustworthy, CA raise an alarm and inform the nodes within its range.

K S Arathy et al. [16] discuss the scheme for detecting single and multiple BH attacks. Three additional concepts are used to detect single and multiple BH attacks. These concepts are fake RREQ with a fake / nonexistent destination address, single BH and collaborative BH nodes. Average destination sequence number (ADSN) is calculated which is treated as threshold for destination sequence number. Source node will announce RREQ with fake destination number. Legitimate nodes does not reply with fake route requests. So any node replied to that fake RREQ packet will be considered as malicious node and added to the BH list. Malicious nodes also reply with highest sequence to attract more traffic towards itself. For this purpose, every destination sequence number in RREP packet will be compared with ADSN. DSN (destination sequence number) must be smaller than ADSN. If the DSN is smaller than ADSN, the next algorithm for Collaborative BH attack will be invoked. In detection of collaborative BH attack, the RREP generated node must include it next hop node in RREP. If the replied node or its NHN already in BH list, the RREP will be immediately discarded. Both the nodes will be added to collaborative BH list. If the DSN of the replying node is greater than ADSN, both replied and its NHN will be declare as malicious and added to the BH list.

Patel Bhoomika D. et al. explained the idea in [17]. There are two types of nodes called generic and gateway nodes in WSN. Generic nodes are multipurpose nodes used for

sensing, computing and processing while gateway nodes are used for routing. Random ranks assigned to every node. Node's ranks will be increased if a node successfully forward data packets in the previous events, otherwise decrease. When the rank dropped to zero, it will be considered as an attack. Trust of a node is calculated as the product of rank, remaining battery power and stability factor. In paper [18] Prachi Dewal et al. proposed the scheme for detecting and preventing BH attacks in cluster based WSN. Network is divided into clusters and two CH will be selected from each cluster. CH's will maintain a list, where the node ID's will be saved. Threshold is defined so the nodes should send their data within due time. A node failed to send information within time will be declared as a BH and hence removed. BS is responsible to monitor the CH's. BS will wait to receive the packets from CH. If CH did not send any packet within due time, BS will declare the CH as a malicious node. BS will raise an alarm and alert the network. The second CH will be activated and the nodes will be connected to second CH.

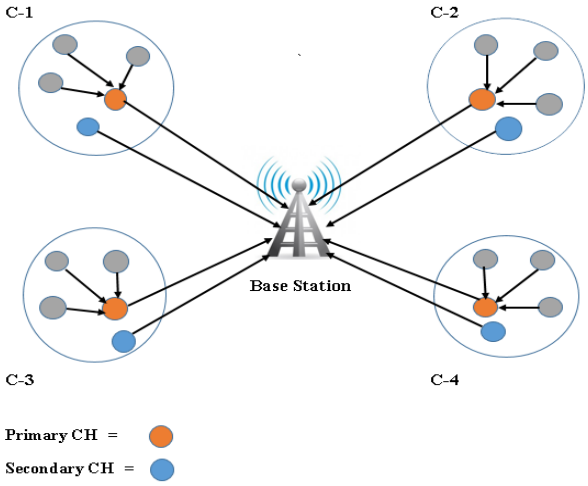

Figure 4: Two CH's approach [18]

Reem Alattas [19] proposed a scheme to detect BH attack by using multiple base station and check agents. Every node is maintaining a table of its neighbour nodes. In the network special nodes called check agents are inserted. Check agents visit every node and monitor the flow of incoming and outgoing traffic. If the frequency of incoming and outgoing packets equal to zero, that node will be declared as suspicious node. To further confirm the maliciousness of a node, multiple base station algorithm is executed. Multiple base stations will send route request or data packet to the suspected node. Node should reply within the threshold time, otherwise it will be considered malicious and removed from the network. In [20] Muhammad Umar Farooq et al. presented the concept for detecting BH attacks by considering energy preservations model. The sensor network divided into clusters, a CH is selected. CH assign ID's to sensor nodes and is responsible to detect the malicious nodes. BS is responsible to elect a CH and monitor its behaviour. BS send AP (authentication packets) to the CH. The AP consists of ID of the CH, Seq Nnumber and Authentication bit. In reply the CH sends RP (Reply Packet) to verify its authenticity. The RP contains the sender ID, sequence number and Ack Bit. Similarly CH sends a AP to the sensor node having sensor's node ID, sensor node Seq number and authentication bit to verify the authenticity of the node. Sensor node reply with RP having its ID, Seq number and Ack Bit (Ack bit is incremented by one of authentication bit). In normal flow, sensors nodes sending DP's (Data Packets) to the CH. DP's contain the ID and Seq number of the Sender node. Malicious cannot send DP's to the CH. CH waits for a specific period of time and if it does not receive any packet, it will mark that particular node as a BH node. CH remove those nodes from the routing table and rearrange it's cluster. BS is collecting data from CH's and wait for a specific amount of time. CH must send the data within time. If the CH failed to send the packets within due time will be marked as a BH node. BS will send stop packet to the nodes. After receiving the stop packet, nodes will stop further communication.CH selection algorithm will be called to select a new CH.

Zeba Ishaq et al. [21] presenting the framework for detecting malicious nodes in cluster based WSN. The proposed framework divided into three levels. In first level CH, IN (inspector node) and MN's (sensor nodes) are selected. Every sensor node can be selected as a CH. For CH selection, nodes will broadcast the requests to their neighbors. If 70 % nodes satisfied then the CH will be selected For IN selection the CH requested the sensor nodes to participate and randomly selects the inspector node. IN should be reachable by the CH. All nodes are maintaining reputation of its neighbor nodes, IN and CH. Good and bad reputation of a node totally depends upon the ability to communicate and forwarding data. CH will assign Initial reputation values to inspector, member, other CH's and gateway nodes. Each node can decide of their own to select only good reputation nodes for data forwarding. Inspector nodes monitor the activities of CH and MN to detect the malicious nodes. CH randomly send requests to check that the IN is active or not. IN must respond to the CH messages.

Jagadeesh Kakarla et al. proposed the trust base scheme for BH and gray hole attacks in WSN [22]. The network is divided into clusters and CH is selected for each cluster. All sensor nodes oversee their neighbors and computing their trust values. The confidence of a sensor node on its neighbor depends upon its past interactions. Keeping the history will help the nodes to calculate trust values for their neighbors. The calculated trust values are also send to the CH. CH use these values to calculate total trust of every node and shared the result with its cluster members. Initially sensor nodes assigned a value of 0.5 which is updated in a regular fashion. When a node successfully transmit the packets, its reputation increased otherwise decreased. Only high trust nodes will be selected for data transmission. The node having a lower trust value will be avoided to improve network performance. In paper [23] Pooja Dr. et al discuss an assessment based approach for detecting BH attacks. Every node computing hint values for other nodes and store them. Hint value is basically the time between a connection established and connection break. There is also a threshold value. The hint

value is then compare with the threshold (TH) value. Hint values less than the threshold will be marked as malicious nodes. The values greater than the threshold, will be declared as a normal node. In this approach the nodes with higher hint values will be selected for routing data. This will decrease the chances of attacks like black hole.

A. Babu Karuppiah et al. proposed the approach for detecting BH attacks in WSN [24]. Network consists of BS, CH, agent and sensor nodes. At the end of every communication session, nodes will send a CP (control packet) to the CH and agent. CP consists of node ID and total number of packets sent. CH and agent will forward the control packet to the BS. BS compares the packets received from CH with number of packets in CP. If the BS found any difference between the received packets in the CP and packets forwarded by CH. The CH will be declared as black hole. BS will alert the network by using ID of the malicious node. Every node is maintaining a table, where they put the malicious node ID's. This table can be used for selection of CH. if the ID advertised for CH included in BH table, they will discard that reply. This approach ensures that a malicious node cannot be selected as a CH.

In [25] Han-Chao Lee et al. detected unfaithful nodes by implementing the responsive probing strategy. In this mechanism encrypted probe packets are injecting in normal data packets. Malicious nodes can be detected by using degree of misbehaving intrusion (DMI). DMI is calculated as the value of source node, destination node and time defined. The zero value of DMI indicating a normal flow. Probing packets send within a pre-defined schedule. Malicious nodes can be identified by its behavior like dropping, blocking and delaying. Source node will send probe packets towards destination. The probing strategy applied to calculate the DMI value. Destination node will wait for specific time (threshold) to receive probe packets. If the destination node did not receive probe packets, it will calculate DMI for source – destination node. DMI greater than zero will be considered that a bad node is present. DMI value is helpful to figure out malicious path / nodes. The destination node will broadcast node ID of the malicious node into the network.

III. COMPARATIVE ANALYSIS

The purpose of this study is to observe and compare different schemes proposed for detecting and preventing black hole attacks. We analyse each technique and discuss its positive and negative aspects. Final analysis is shown in the Table *1*.

In paper [1], the network is divided into clusters which is a good approach. Due to clustering sensor nodes will only sent the data to the CH. the overhead, congestion, energy consumption and data redundancy will be decreased. Mobile agents are visiting each node to observe its behaviour, which provides real time monitoring. No results for end – to – end delay and PDR is given. It is not clearly define that for how long the agent will stay at each node. In paper [2], sensor are able to select an alternative path if a bad node is detected. Sensor nodes can be identified by its unique ID's. Using IDS on each node provides real time monitoring and any malicious activity will be reported on time. AODV protocol is a reactive protocol which favours energy constrained devices. Network congestion may be created due to absence of clustering. Using IDS on every node may use the node's energy. In [3] the author assuming cryptographic solutions to secure link security. Information will travel through high trust nodes only but who will maintain the trust value of nodes, it's not clear. Looking for a new route may consume time and extra energy as well. Each node is also sending individual information so a network congestion may also occur. In paper [4] the author use the concept of trust to figure out black hole nodes. Clustering is minimizing energy consumption, overhead and redundancy of data. CH is maintaining trust table, so it is easy to filter good and bad nodes. The black hole attack can be detected, BS should alert the network about the malicious node.

In [6], the working principle of honey bee colony implemented. The decision is based on RREP packet. If a node reply to RREQ, then the source will start transmitting data. Malicious node always reply with a fake RREP that it has the smallest route to the destination. There is no such mechanism defined to prevent this type of attack. In paper [7], the concept of clustering will decrease the overhead, and network congestion. Malicious node can be easily identified by using node ID's. The author proposed that sensor nodes should send the data to all routers. This will increase network complexity, more energy consumption so clustering may not work as efficient as it should be. In paper [8], all nodes managing their own tables to know the reputation and legitimacy of other nodes. This approach seems good because it can easily identify bad nodes if the trust value become less than the threshold. On the other side it is not clear that how many values a table can store. Using Digital signature scheme and maintaining a large table, there will be more overhead and energy consumption on each node.

In paper [10] trust model is used to detect the malicious nodes, the technique seems good but other factors like energy and overhead should also be considered. All nodes are responsible to calculate the functional reputation of its neighbours. Nodes calculations will consume extra energy. Storing values and sharing this information with other nodes will increase overhead on nodes. In [11], the approach based on reply and time limit. Malicious nodes always pretend that they have a shortest path to the target node. No such mechanism discussed to differentiate between legitimate and malicious node replies. In [12] the author propose a very efficient scheme for detecting black hole attacks. All nodes should be register with base station. Base Stations store the energy levels, the CH is selected based on highest energy. In re-clustering a new node will be selected as CH. If an existing CH participated again, its current energy level will be compared with its previous level. If the energy level is same as previous, that node will be marked as suspicious node. False positive chance are present there. In [13] the authenticity of the nodes is verified so only legitimate nodes can participate in communication process. The key renewal scheme is keeping the trust level, but for how long not clear.

The authentication mechanism and its impact on energy and overhead is not defined. In paper [14] an efficient work has been proposed for detecting black hole nodes. Throughput improved but the delay and packet overhead is more because of using extra packets.

In [15] RSA public key cryptographic solution is implemented. Sensor nodes are very limited in energy, processing and computations, they will not survive for a longer period of time. Overhead and energy consumption will be increase due to complex computations. In [16], the network is flooded with fake RREQ packets. The network will be overladed because every node is tested. Security approach discussed in [18] provides real time monitoring. Clustering is used so energy and overhead issues can be minimized. A malicious node always claiming highest energy to become a CH. No procedure defined to detect a node, claiming the highest energy over and over again. In [19] the author deployed check agents. Check agents are self – organized piece of software, used to monitor node's activity. Every node is maintaining a list of neighbouring nodes. This approach detect the black hole attacks but if the number of BH nodes are high, the probability of detection decreases. In [20] the authors proposed the authentication model b/w CH's and BS. Authentication is a good option to differentiate between legitimate and illegitimate nodes. In this model Throughput and packet delivery ratio increased, while energy consumption and end-to-end delay decreased. Overhead depends on the complexity of authentication mechanism. CH selection process needs improvement. A malicious node always announce that it has the highest energy. No mechanism is defined in the paper to address this issue.

In [21] a security framework for detecting selfish node is proposed. The approach is detecting the bad nodes but lacks in other areas. In this approach each node has the option to become a CH. CH is selected based on the trust shown by neighbour nodes. How other nodes should trust this because they don't know about the node's energy level and its legitimacy. In the second phase each node is calculating the trust values of other nodes. The results show that packets drop minimized and throughput improved. No results available for PDR and End-To-End delay. All nodes are monitoring every message of the CH, sent to sink. So nodes will consume more energy to listen every packet hence the overhead ratio will be high as well.

Table 1. Comparative Analysis of Existing Techniques

S. No	Approaches / Schemes	Energy Cons	Overhead	PDR	Throughput	E – E – D	Tool
1	BHDZBWSN	L	L	N/A	M	H	NS2
2	DPBHWSN	H	H	I	I	M	Ns-2.35
3	ISDBHWSN	H	H	H	H	L	NS
4	HTB-BHD-SG	L	L	H	H	L	NS – 3
5	GTBSM-BHON	H	M	H	L	L	One
6	EPDOSD	-	-	I	I	L	NS
7	FM-DPBH-WSN	H	M	H	H	L	—
8	CRCMD&R	H	H	H	H	H	Mat-lab
9	HTB-IDS-WSN	H	H	H	L	H	OMNET++
10	DIBH-WSN-HT	H	H	H	H	L	—
11	DPBH-WSN	L	L	I	H	L	QualNet
12	EDRI-DE-CBH	H	H	H	H	L	Opnet 14
13	FT-DBH	H	H	H	L / M	L / M	MATLAB
14	NDSCBH	M / H	L / M	H	M / H	L	N/A
15	TBS-DNW-WSN	H	L / M	I	I	M	NS2
16	DPBH-CBWSN	L	L	—	—	—	—
17	DBHWSN-MBSCA	H	H	H	M / H	H	OMNet ++
18	EPDM-CBH	L	M / H	H	H	L	NS2
19	SF-CBWSN	H	H	H	I	M / H	MATLAB
20	TBSCM-WSN	H	H	H	H	L	NS2
21	ABA-DBHA	H	L / H	M / H	M / H	H	ONE
22	IH-BHDA-WSN	L	I	NC	NC	NC	NS2, C++
23	RPA-DDI-MANET	H	H on DN	I	I	L / M	NS2

Table 2. Explanation of Acronyms used in Table 1

S. No	Acronym Used	Meaning
1	L	Low
2	M	Medium
3	H	High
4	I	Improved
5	DN	Destination Node
6	PDR	Packet Delivery Ratio
7	E – E – D	End to End Delay
8	NC	No Change
9	BHDZBWSN	BH Attack detection in Zone based WSN
10	DPBHWSN	Detection and Prevention of BH Attack in WSN Using Ns-2.35 Simulator

11	ISDBHWSN	Improving Security and Detecting BH attack in WSN
12	HTB-BHD-SG	Hierarchical Trust Based, Black Hole Detection in WSN based Smart Grid Monitoring
13	GTBSM-BHON	A game theory based secure model against BH attacks in Opportunistic Networks
14	EPDOSD	An Effective Performance For Denial Of Service Attack (DoS) Detection
15	FM-DPBH-WSN	Futuristic Method to Detect and Prevent BH Attack in WSN
16	CRCMD&R	Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme
17	HTB-IDS-WSN	A Hybrid Trust Based IDS for WSN
18	DIBH-WSN-HT	Detection and Isolation of BH attack in WSN using Hybrid Technique
19	DPBH-WSN	Detection and Prevention of BH Attacks in WSN
20	K3TM-ID-WSN	A Key-Based 2 Tier Trust Management Filtering Scheme for Intrusion Detection in WSN
21	EDRI-DE-CBH	An EDRI-based approach for detecting and eliminating cooperative BH nodes in MANET
22	FT-DBH	Fuzzy Trust Approach for Detecting Black Hole Attack in MANET's
23	NDSCBH	A Novel Approach for Detection of Single and Collaborative BH Attacks in MANET
24	TBS-DNW-WSN	A Trust Based Solution for Detection of Network Layer Attacks in WSN
25	DPBH-CBWSN	Detection & prevention of BH attacks in cluster based WSN
26	DBHWSN-MBSCA	Detecting BH Attacks in WSNs using Multiple Base Stations and Check Agents
27	EPDM-CBH	Energy Preserving Detection Model for Collaborative Black Hole Attacks in WSN
28	SF-CBWSN	A Security Framework for Cluster-based WSN's Against the Selfishness Problem
29	TBSCM-WSN	A Trust Based Secured Coordination Mechanism for WSAN
30	ABA-DBHA	An Assessment Based Approach to Detect BH Attack in MANET
31	IH-BHDA-WSN	An Improvised Hierarchical BH Detection Algorithm in WSN
32	RPA-DDI-MANET	A Responsive Probing Approach to Detect Dynamic Intrusion in a MANET

IV. Conclusion and Future work

WSN are emerging at a rapid pace and many technologies are adopting them. WSN are low cost, small in size, intelligent and easy to deploy. Sensor devices come up with very limited processing, computing and battery power. Conventional cryptographic solution cannot be implemented in sensor nodes. Due to these limitations, Wireless Sensor Networks are open to many security attacks. Out of these threats, Black hole is the most dangerous attack. A network compromised by Black Hole attack may lead to huge energy losses, congestion and network overhead issues. Black hole attack significantly affect the network performance. We discussed and compared different schemes i.e. Hierarchical, trust based, multi hop, check agents and secure routing. These solutions are good, but most of them are designed for a specific purpose. New techniques should be develop while considering the energy, processing and computation power of WSN nodes. The current techniques also requires further improvements because there lies a number of flaws. In future WSN will be deployed almost everywhere, so comprehensive work is required to reduce the risk of BH attacks.

V. References

[1] Dr. Shreenath K N, Manasa V M "Black Hole Attack detection in Zone based WSN" International Journal on Recent and Innovation Trends in Computing and Communication, pp 148–151, Volume:5, Issue:4, April 2017

[2] Abhinav Kaurav, Kakelli Anil Kumar, "Detection and Prevention of Black hole Attack in Wireless Sensor Network Using Ns-2.35 Simulator" IJSR CSEIT, Volume 2 | Issue 3, May – June 2017

[3] Pavan Kumar Gupta, M. Madhu, "Improving Security and Detecting Black Hole Attack in Wireless Sensing Networks" International Journal of Professional Engineering Studies, Vol VIII, Issue 5, August 2017

[4] Safa Otoum, Burak Kantarci and Hussein T. Mouftah, "Hierarchical Trust Based, Black Hole Detection in

WSN based Smart Grids" IEEE, international conference on Communications (ICC), Paris, France, pp 1 – 6, 21-25 May 2017

[5] Anshuman Chhabra, Vidushi Vashishth and Deepak Kumar Sharma, "A game theory based secure model against Black hole attacks in Opportunistic Networks" IEEE, Information Sciences and Systems (CISS), pp 1 – 6, Baltimore, MD, USA, 22-24 March 2017

[6] P. Hemalatha, J. Vijithaananthi, "An Effective Performance For Denial Of Service Attack (DoS) Detection" IEEE, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)", pp 229 – 233, Palladam, India, 10 – 11 February 2017

[7] Abdullah Aljumah, Tariq Ahamed Ahanger, "Futuristic Method to Detect and Prevent Black-Hole Attack in Wireless Sensor Networks" IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.2, 05 February 2017

[8] Saurabh Sharma, Dr. Sapna Gambhir, "CRCMD&R: Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme in MANETs", IEEE, 11th International Conference on Intelligent Systems and Control (ISCO), pp 36 – 340, Coimbatore, India, 5-6 January 2017

[9] Christiana Ioannou, Vasos Vassiliou and Charalampos Sergiou "An Intrusion Detection System for Wireless Sensor Networks" IEEE, 24th International Conference on Telecommunications (ICT), pp 1 – 5, Limassol, Cyprus, 3-5 May 2017

[10] Mert Melih Ozcelik, Erdal Irmak, Suat Ozdemir "A Hybrid Trust Based IDS for WSN" IEEE, Networks, Computers and Communications (ISNCC), pp 1 – 6, Marrakech, Morocco, 16-18 May 2017

[11] Arshdeep Kaur "Detection and Isolation of Black hole Attack in WSN using Hybrid Technique (Received and Time Delay)" IEEE, International Conference on Inventive Computation Technologies (ICICT), pp 1 – 5, Volume: 2, Coimbatore, India, 26-27 August 2016

[12] Gurjinder Kaur1, V.K. Jain, Yogesh Chaba "Detection and Prevention of Black hole Attacks in WSN" Springer, International Conference on Intelligent, Secure, Dependable Systems in Distributed and Cloud Environments (ISDDC), pp 118-126, Vancouver, BC, Canada, 25-27 October 2017

[13] Moutushi Singh, Rupayan Das, Mrinal Kanti Sarkar, Koushik Majumder and Subir Kumar Sarkar "A Key-Based Two-Tier Trust Management Filtering Scheme for Intrusion Detection in WSN" Springer, Proceedings of the Second International Conference on Computer and Communication Technologies, pp 679-690, Volume 1, Springer India, January 2016

[14] Ali Dorri "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET" Springer Wireless Networks New York, Volume 23, Issue 6, pp 1767–1778, Springer US, Aug 2017

[15] G. Arulkumaran, R. K. Gnanamurthy "Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network" Springer

Mobile Network and Applications, pp 1–8, Springer US, Sep 2017, ISSN: 1572-8153

[16] K S Arathy, C N Sminesh "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET" Elsevier Procedia Technology Volume 25, Pages 264-271, Sep 2016

[17] Patel Bhoomika D., Patel Ashish D. "A Trust Based Solution for Detection of Network Layer Attacks in Sensor Networks" IEEE, International Conference on Micro Electronics and Telecommunication Engineering, pp 121 – 126, Ghaziabad India, 22-23 Sep 2016

[18] Prachi Dewal, Gagandeep Singh Narula, Vishal Jain "Detection and prevention of black hole attacks in cluster based wireless sensor networks" IEEE, 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp 3399 – 3403, New Delhi India, 16-18 March 2016

[19] Reem Alattas "Detecting Black-Hole Attacks in WSNs using Multiple Base Stations and Check Agents" IEEE, Future Technologies Conference, pp 1020 – 1024, San Francisco, CA, USA, 6 - 7 Dec 2016

[20] Muhammad Umar Farooq, Xingfu Wang, Robail Yasrab, Sara Qaisar "Energy Preserving Detection Model for Collaborative Black Hole Attacks in Wireless Sensor Networks" IEEE, 12th International Conference on Mobile Ad-Hoc and Sensor Networks, pp 395 – 399, Hefei, China, December 2016

[21] Zeba Ishaq, Seongjin Park and Younghwan Yoo "A Security Framework for Cluster-based WSN's Against the Selfishness Problem" IEEE, Seventh International Conference on Ubiquitous and Future Networks (ICUFN), pp 7 – 12, Sapporo Japan, 7-10 July 2015, ISSN: 2165-8536

[22] Jagadeesh Kakarla, Banshidhar Majhi, Ramesh Babu B "A Trust Based Secured Coordination Mechanism for WSAN" IEEE, International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), pp 1 – 5, Kozhikode India, 19-21 February 2015

[23] Pooja, Dr. R. K. Chauhan "An Assessment Based Approach to Detect Black Hole Attack" IEEE, International Conference on Computing, Communication and Automation (ICCCA), pp 552 – 557, Noida India, 15-16 May 2015

[24] A. Babu Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram "An Improvised Hierarchical Black Hole Detection Algorithm In Wireless Sensor Networks" IEEE, International Conference on Innovation Information in Computing Technologies (ICIICT), pp 1 – 7, Chennai India, 19-20 Feb 2015

[25] Han-Chao Lee, Shin-Ming Cheng , Kuo-Ping Wu1, Hahn-Ming Lee "A Responsive Probing Approach to Detect Dynamic Intrusion in a MANET" IEEE, 7th International Conference on Information, Intelligence, Systems & Applications (IISA), pp 1 – 6, Chalkidiki Greece, 13 – 15 July 2016

[26] Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, Nazar A. Saqib "Detection and Prevention of Distributed Denial of Service Attacks in VANET's", International Conference on Computational Science and Computational Intelligence (CSCI), pp 970 – 974, Las Vegas, NV, USA, 15-17 Dec. 2016

[27] Samera Batool, Nazar A. Saqib, Muazzam. A. Khan, "Internet of Things data analytics for user authentication and activity recognition", 2nd International Conference on Fog and Mobile Edge Computing (FMEC), pp 183 – 187, Valencia, Spain, 8-11 May 2017