BHnFDIA : Energy Efficient Elimination of Black Hole and False Data Injection Attacks in Wireless Sensor Networks

Tanuja R
Bangalore University
Dept. of Computer Science
UVCE, Bangalore

S H Manjula
Bangalore University
Dept of Computer Science
UVCE, Bangalore

K R Venugopal
Bangalore University
Department of Computer Science
UVCE, Bangalore

L M Patnaik
Indian Institute of Science
Bangalore
India

ABSTRACT

Wireless Sensor Networks (WSNs) are currently being used in a wide range of applications including military areas that demand high security requirements. WSNs are susceptible to various types of attacks as they are unsupervised in nature. Since sensor network is highly resource constrained, providing security to data transmission becomes a challenging issue. Attacks must be detected and eliminated from the network as early as possible to enhance the rate of successful transmissions. In this paper, an energy efficient algorithm is proposed to eliminate Black Hole and False Data Injection Attack (BHnFDIA) to overcome black hole attack in WSNs using a new acknowledgement based scheme with less overhead. Every intermediate node check the authenticity and integrity of the received packet. The authentic packets will be forwarded and malicious packets will be discarded immediately. The proposed scheme can eliminate false data injection by outside malicious nodes and Black hole attack by compromised insider nodes. Simulation results show that the scheme can successfully identify and eliminate 100% black hole nodes. Malicious packets are immediately removed with 100% filtering efficiency. The scheme ensures more than 99% packet delivery with increased network traffic.

General Terms:

Wireless Sensor networks, Security

Keywords:

ACK_SINK (Sink Acknowledgement), Black hole attack, False data injection, Packet delivery rate, Security in WSN

1. INTRODUCTION

A Wireless Sensor Network typically consists of a few to several hundreds or even thousands of sensor nodes. These sensor nodes are spatially distributed in an autonomous fashion. The main components of a sensor node are the following: microcontroller, transceiver, external memory, power source and one or more sensors. These sensor nodes are usually deployed in harsh, unattended, remote areas and have limited sensing, computation and communication capabilities. The sensor networks are often exposed to various malicious attacks and the conventional defense mechanisms are not suitable because of its highly resource constrained nature. Hence security in WSNs becomes a crucial challenge and many research works are anticipating in this area.

Today WSNs have wide range of applications. Sensors can be deployed for environmental monitoring including forest fire detection, air pollution monitoring, oceanographic data collection and green house monitoring. Sensors are used in industrial monitoring and agricultural purposes. Military applications demanding high security include intrusion detection, nuclear and chemical attack detection, perimeter monitoring, battlefield surveillance and battle damage assessment. Healthcare applications include drug administration, patient monitoring and data collection. Advancements in sensor network technology guarantee its use in smart environments and other commercial applications.

Since sensor nodes are densely deployed in unattended, harsh, remote environments, the network is vulnerable to various security attacks: false data injection attacks, passive information gathering, sinkhole attacks, wormhole attacks, message corruption, traffic analysis, DoS attacks and selective forwarding [1]. This paper concentrates on detecting and eliminating an insider attack, called black hole attack, in wireless sensor networks. Black hole attack is a simple form of selective forwarding attack, where a malicious node may drop all the packets passing through it without forwarding to sink node. We also consider false data injection attack from outside malicious nodes where an attacker will inject false data reports into the network and deplete the energy of forwarding nodes.

The existence of various threats and attacks has inspired new research that address the security issues of WSNs. Most of the current research security areas can be categorized into the following four categories

—Key management: Establishing and maintaining cryptographic keys in an energy efficient manner to provide secure communication. There are two fundamental key management schemes for WSNs: static and dynamic.

—Secure routing: For new routing protocols applying security measures, without sacrificing network connectivity or scalability.

—Secure services: Includes specialized security services such as data aggregation, localization and time synchronization.

—Intrusion Detection Systems: Detect specific attacks and provide counter measures without consuming excessive amount of energy or memory.

$Motivation$: For security, the data sensed and transmitted by the sensor nodes must reach the destination sink node and the information must be authentic and accurate. The security mechanisms should be strong enough and undoubtedly energy-efficient to prevent attacks by malicious nodes to reduce the wastage of sensor resources and to provide authentication and integrity to sensed data. Attacks in wireless senssor networks are broadly classified into insider and outsider attacks. The outsider attacks can easily be detected and healed using some cryptographic mechanisms. But for insider attacks, the cryptographic schemes are ineffective because the compromised nodes have all the private details of the node including cryptograhic keys.

Since reducing communication cost is an important challenge in securing WSNs, [2] proposed an energy-efficient secure framework suitable for resource constrained wireless networks which can overcome false data injection by outside malicious node. But it does not address insider attacks. The purpose of this paper is to detect and overcome black hole attack by compromised insider node and also incorporates false data injection attack by outside malicious node.

$Contributions$: This paper can overcome black hole attack in wireless sensor networks using a new acknowledgement-based detection scheme. This will increase the packet delivery rate. Our scheme can also eliminate false data injection attacks from outside malicious nodes. Our framework does not require exchange of control messages for key refreshment in normal behaviour. But when re-routing is required, the black hole detecting node will send records to its neighbours in the new route to maintain synchronization with nodes in the downstream direction. Since MAC is not appended to the packet, packet size will not be enlarged. Unique keys are used for transmission of each packet.

$Organization$: The remaining part of the paper is organized as follows: Related Works is presented in section 2. BackGround is discussed in section 3. Network Model is presented in section 4. Section 5 describes Problem Definition and Algorithm. Implementation and Performance Evaluation is shown in section 6. Finally, section 7 gives the conclusions of the paper.

2. RELATED WORKS

Zia and Zomaya [1] have made effort to document the security issues in WSNs. Attacks, countermeasures and threat models have been proposed in different layers. Arif et al., [2] have designed Virtual Energy-Based Encryption and Keying (VEBEK) scheme, resulting in reduced number of overhead messages thereby increasing the lifetime of WSNs. The intermediate nodes can verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the senders virtual energy, thus requiring no need for specific rekeying messages. It uses one key per message for successive packet transmissions. This ensures the elimination of malicious data from the network. The performance shows 60-100 percent improvement in energy savings over other schemes such as DEF, SEF and STEF. This work does not address insider attacks and dynamic paths.

Misra et al., [3] have proposed an efficient technique, BAMBi, to mitigate the adverse effects of black hole attacks on WSNs. This scheme uses multiple base stations deployed in the network to counter the impact of black holes on data transmission. BAMBi requires very little computation and message exchanges in the network, thus saving the energy of the SNs. This technique offers more than 99% packet delivery success, suffers from very little false positives and can identify 100% black hole nodes in the network.

Bysani and Turuk [4] have discussed about selective forwarding attack, its types and some mitigation schemes to defend such attacks. Kaplantzis et al., [5] have proposed a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and sliding windows. It uses only two features to detect selective forwarding and black hole attacks. This IDS uses routing information local to the base station of the network and raises alarms based on the 2D feature vector (bandwidth, hop count). Classification of the data patterns is performed using a one-class SVM classifier. This system can detect black hole attack with 100% accuracy and selective forwarding attacks in which 80% of the network is ignored with 85% accuracy. Since intrusion detection is performed at the base station sensor nodes expend no energy to support this security feature.

Yu and Yong [6] have proposed a dynamic en-route quarantine scheme - Hill Climbing key dissemination approach - using hash chain of authentication keys to overcome false data injection attacks and DOS attacks in dynamic WSNs. This scheme drops false reports much earlier with a smaller size of memory. The uncompromised nodes cannot be impersonated and the memory requirement is balanced. This scheme also mitigates the impact of selective forwarding attacks. The compromised nodes have no way to contaminate legitimate reports or generate false control messages. It requires extra control messages, increases operation complexity, triples the delay of reports, increases memory overhead of the forwarding nodes and cannot coordinate with other energy efficient protocols. The control messages can also be attacked. This scheme can drop false reports in 6 hops with only 25 keys stored in each node, while another scheme needs 12 hops even with 50 keys stored.

Hou et al., [7] have presented the Dynamic Energy-based Encoding and Filtering framework (DEEF) to detect the injection of false data into a sensor network by encoding data using the results of a keyed hash. The key to the hashing function dynamically changes as a function of the transient energy of the sensor and thus there is no need to refresh keys. DEEF can eliminate 90% - 99% of false data injected from an outsider within 9 hops before it reaches the sink, without increasing transmission overhead. DEEF-T and DEEF-NT can be configured to provide optimal performance in a variety of network configurations. DEEF leads to synchronization problems due to fluctuations in battery levels which can cause packet drops.

Selcuk et al., [8] have presented the Time-Based Dynamic keying and En-Route Filtering (TICK) protocol for WSNs to send events to the sink in an energy-efficient and secure manner, without sending rekeying messages. Sensor nodes use their local time values as a one-time dynamic key to encrypt each message. TICK consumes less energy when compared to other schemes like DEF,

Table 1. **Comparison of Various Works**

Author	*Protocol*	*Concept*	*Advantage*	*Performance*
Kaplantzis et al.,	Centralized intrusion detection scheme based on Support Vector Machines (SVMs) and sliding windows.	Uses routing information local to the base station of the network and raises alarms based on the 2D feature vector.	Detect black holes and selective forwarding attacks with high accuracy without depleting energy of sensor nodes.	Detect black hole attack with 100% accuracy and selective forwarding attacks in which 80% of the network is ignored with 85% accuracy.
Misra et al.,	Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks.	Uses multiple base stations deployed in the network to counter the impact of black holes on data transmission.	Requires very little computation and message exchanges in the network.	Ensures 99% packet delivery success, suffers from very little false positives and can identify 100% black hole nodes in the network.
Hou et al.,	Dynamic Energy-based Encoding and Filtering Framework.	Detect the injection of false data by encoding data using the results of a keyed hash.	Can be configured to provide optimal performance in a variety of network configurations. No need to refresh keys.	Eliminate 90%-99% of false data injected from an outsider within 9 hops before it reaches the sink.
Selcuk et al.,	TIme-Based DynamiC Keying and En-Route Filtering protocol.	Send events to the sink in an energy-efficient and secure manner without rekeying messages using local time values as one-time dynamic keys.	Consumes less energy when compared to DEF, SEF and STEF. Prevents malicious nodes from injecting false data into the network.	Malicious packets are immediately taken out from the network.
Arif et al.,	Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks.	Key management scheme that reduces number of transmissions needed for rekeying thereby increasing the lifetime of sensor network.	Consumes less energy when compared to DEF, SEF and STEF. Ensures the elimination of malicious data from the network.	Overall 60%-100% improvement in energy savings when compared to other schemes in the literature.
Our Scheme	Black hole Detection and Elimination Algorithm (BHnFDIA).	Detect and eliminate black hole attack using a new acknowledgement based detection scheme. Also filter false data injection by outside malicious nodes.	Ensures the elimination of false data injected by outside malicious nodes with less energy consumption. Increases successful packet delivery rate by removing black holes.	Malicious packets removed within one hop with 100% filtering efficiency. Successfully identify and eliminate 100% black hole nodes. Ensures 99% packet delivery with increased packet count.

SEF, STEF and TPSKD. TICK prevents malicious nodes form injecting false data into the network. The insider attacks are not addressed in this work.

Lin et al., [9] have presented Energy-efficient Location-dependent key management scheme (ELKM) to improve the performance of LDK. ELKM generates keys for each node based on their relative locations. Based on loose time synchronization, ELKM reduces energy consumption by minimizing the total size of transmitted message during establishment of secure links. It provides high security level by reducing the exposure of key materials to adversaries and guarantees good network connectivity. ELKM consumes about $1.2x10^4$ mAs energy to achieve the 0.9 network connectivity while LDK consumes about $2x10^4$, which is approximately 2 times of that of ELKM.

Ba et al., [10] have proposed a deterministic key management scheme, DKS-LEACH, to secure LEACH protocol against malicious attacks. Dynamic cryptographic keys are established in an autonomous manner to secure the communications between simple nodes and cluster head as well as the communication between cluster heads and base station. The overhead incurred by DKS-LEACH compared to LEACH is small. It allows level-off the energy consumption and the end-to-end delay and minimize memory usage by using limited number of keys. It prevents the election of untrustworthy cluster heads.

Hu et al., [11] have proposed a robust authentication scheme, RAS, based on a partition-overlapping key pool scheme, for filtering false data in WSNs. To achieve better filtering capacity RAS employs both dynamic authentication tokens from one-way hash chain and secret keys pre-loaded from the key pool for report endorsement. The compromised nodes, even in possession of all endorsement keys cannot modify reports. Attacker has to compromise all T source nodes endorsing the report and to start a new report delivery process while exposing injector ids to make RAS ineffective. RAS can drop 90% false reports within 6 hops when the SEF needs 10 hops.

Kraub et al., [12] have proposed a Secure Ticket-based En-route Filtering Scheme (STEF), addressing false data injection and PDoS attack, applicable in high density resource constrained WSNs. Reply messages with valid tickets issued by base station are forwarded to sink while others are filtered out immediately. STEF performs en-route filtering without symmetric key sharing between sensor nodes and enables the separation of report generation with sink verification resulting in high resiliency against node compromises. Node compromises are limited to the vicinity of the compromised nodes and do not affect the whole network. The storage capacity requirement on the sensor nodes is very low and

energy savings increase with the number of injected false messages and with the distance to the sink where an adversary injects false messages.

Wang and Wei [13] have designed an en-route filtering mechanism with immediately lightweight authentication to defend false data injection, PDoS attacks and collusion attacks. The authorization polynomial function enables intermediate nodes to verify the correctness of the packets, to take decision to reject or transmit reports to next node and to solve time asynchronous problem. An adversary who compromises n+1 or more nodes in the transmission path can only calculate the authorization polynomial function. The storage requirement is practical and acceptable under the existent sensor nodes, which can offer 4 KB of SRAM.

Yuan et al., [14] have proposed KAEF, a one-way key chain authentication based en-route filtering scheme, for WSNs, to overcome false data injection attacks. Each sensor node stores one-way key chain for endorsing reports and each cluster head sends the key chain commitments to the sink. KAEF localizes the influence of node compromise on filtering false reports into one cluster and the use of one-way key chains prevent the adversary from replaying legitimate reports. KAEF detects and discards 90% of false reports within 22 hops while SEF achieves the same detected fraction within 45 hops in its worst case where number of compromised nodes is 4. When a report traverses 100 hops, about 40%of energy is saved by KAEF as compared to the case without en-route filtering mechanism, while the fraction of energy savings by SEF is only about 20%.

Ren et al., [15] have designed a location-aware end-to-end security framework (LEDS) to overcome DoS attacks by exploiting the static and location aware nature of WSNs. Secret keys are bound to geographic locations and each node stores a few keys based on its own location to limit the impact of compromised nodes only to their vicinity without affecting end-to-end data security. Multi-functional key management framework assures both node-to-sink and node-to-node authentication along the report forwarding routes and data delivery approach guarantees efficient en-route bogus data filtering. LEDS achieves 85 percent or more energy savings in contrast to the case without using this design when appropriate parameters are chosen. LEDS only requires the nodes to store a small number of keys, which can be as low as 20, when the number of endorsements is 5 and the number of keys is independent of the network size.

Kim et al., [16] have proposed a cluster adaptation method (CAM) to enhance the filtering efficiency of SEF in sensor networks. A fuzzy rule-based system is used to adjust the cluster regions, considering the conditions of the sensor node and cluster region. CAM organizes efficient cluster regions for SEF, reduces energy consumption for forwarding and makes the event reports as needed. CAM can maintain the cluster regions more efficiently than OCM method and shows good efficiency when the event reporting occurs more than 300 times.

3. BACKGROUND

In dynamic key management schemes, the key refreshment will takes place either periodically or on demand as needed by the network. This will increase the security of the system but, the key refreshment requires the exchange of control messages which will increase communication cost. Rekeying without extra control messages will help to design cost-efficient, secure network protocols for WSNs.

In VEBEK algorithm [2] virtual energy concept is introduced where each sensor node has given a certain virtual energy value when it is first deployed in the network. After deployment sensors may follow different stages: node-stay-alive, sensing, packet reception, transmission, encoding and decoding. The energy costs for these states are represented as $E_{sa}, E_{sens}, E_{rx}, E_{tx}, E_{enc}, E_{dec}$ respectively. Suppose a source node has alive for t units of time since the last event. If that source detects an event, it will send the l-bit packet towards the sink. The virtual cost of the source sensor in this scenario can be represented as:

$$E_c = l * (e_{tx} + e_{enc}) + t * e_{sa} + E_{synch} \quad (1)$$

Here some nodes will keep track of the energy of the sending node called $watching$ operation and the energy associated with the watched sensor is called $Virtual\ Perceived\ Energy$. So, if a receiving node has the intial virtual energy value of the sending node and it successfully receives and decodes packet from a given source sensor K, the virtual perceived energy value can be updated as :

$$E_p^k = l * (e_{rx} + e_{dec} + e_{tx} + e_{enc}) + t * 2 * e_{sa} \quad (2)$$

where in both the equations the small es refer to the one bit energy costs of the associated parameter and the energy for synchronization can be represented as :

$$E_{sync} = l * (e_{rx} + e_{dec}) + e_{sa} * t \quad (3)$$

The cost to transmit data packet at the source node :

$$E_S = E_{sens} + E_{enc} + E_{tx} + E_{sa} \quad (4)$$

The forwarding cost E_{FW} of an intermediate sensor is :

$$E_{FW} = E_{rx} + E_{dec} + E_{enc} + E_{tx} + E_{sa} \quad (5)$$

The framework consists of three modules: Virtual Energy-Based Keying, Crypto and Forwarding modules.The virtual energy-based keying module is responsible for the creation of dynamic keys. The dynamic keys are generated based on the residual virtual energy of the sensor node. Initial key is generated as a function of initial virtual energy and an initialization vector. The subsequent keys are created as a function of current virtual energy and previous key. This key is fed to crypto module. The crypto module provides a simple encoding process. RC4 encryption mechanism is used to generate a permutation code which is used to encode the message. The forwarding module is responsible for sending and receiving of encoded packets along the path to the sink node.

In this paper, the attack detection capability is improved by incorporating black hole attack detection from inside malicious nodes thereby increasing both security and energy efficient packet delivery. Insider attacks are not addressed in [2]. En-route filtering schemes [8] and [14]overcome false data injection but with more energy requirement.

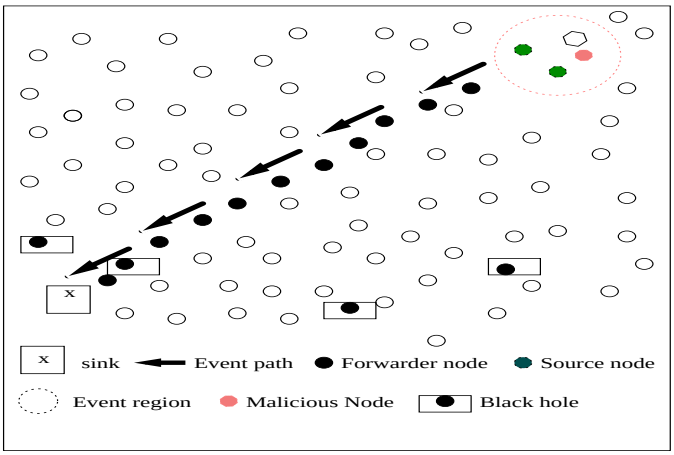

Fig. 1. Network Topology

Table 2. Notations used in the Algorithm.

symbols	*definition*
N	Total no. of nodes in the network
ACK_SINK	Sink Acknowledgement
NACK	Negative Acknowledgement
S	Source
BH	Black Hole
event_ID	Event Identifier
msg	Message
pkt	Packet
t	pre-defined time
FN	Forwarder Node
msgID	Message Identifier
SN	Suspected Node
pc	Permutation Code
msg_X	Message encrypted using X

4. NETWORK MODEL

Consider a typical densely populated wireless sensor network. The topology of the network is shown in Fig. 1. The nodes are randomly distributed in the depolyment region. We assume that sensor nodes remain static after deployment. Given that some event occurs, the nodes detecting that particular event are called source nodes or sensing nodes. They generate and broadcast the sensed report to the sink node. The intermediate nodes between the source node and the sink, forwarding the generated report are called forwarder nodes. False injection and eavesdropping of messages may occur in the network from an outside malicious node. Network may also experience black holes.

Since sensor network is densely deployed, multiple nodes can sense the same event. The routing path between the source node and the sink is assumed to be fixed in the absense of black holes. If black hole is detected, then successive packets will be re-directed. The sensor nodes are assumed to have the same communication ranges and may have same initial battery supplies. All nodes have unique ID.

5. PROBLEM DEFINITION AND ALGORITHM

Since sensor nodes are deployed in harsh, unattended remote areas, they are susceptible to various attacks, both insider and outsider attacks. Outsider attacks can be easily solved using some cryptographic mechanisms. But in the case of insider attacks, after compromising a node, an adversary can access all data including cryptographic keys and can make subsequent attacks as 'legitimate node'. So node-based authentication using cryptographic keys is ineffective in addressing insider attacks.

This paper considers both insider and outsider attacks mainly black hole attack by an insider and false data injection by outside malicious node. Black Hole attack is a type of denial-of-service attack where a node that is responsible for forwarding packets may discard all instead of transmitting. In the attack scenario in this paper, some compromised nodes will act as black holes and drop all the packets passing through it.

5.1 Objectives

(i) To solve black hole attack using a new acknowledgement based detection scheme with less overhead.

(ii) To ensure authenticity and integrity of transmitted packets by preventing false data injection by outside malicious nodes.

5.2 Algorithm

5.2.1 DownStream Process. Downstream represents direction towards sink node. When a source node sense some event, it appends nodeID, type and event_ID along with the sensed data and encode the whole data using virtual energy-based encryption mechanism [2]. Then the source will forward the packet along with its plaintext ID to next hop and wait for a pre-defined time to receive sink acknowledgment, ACK_SINK, from its downstream neighbour. It also stores the event_ID in its own cache until it receives ACK_SINK.

When a forwarder node receives a packet, it authenticates the packet by performing virtual energy-based decoding and compares the plaintext ID with decoded ID. Malicious packets inserted by outsiders will be dropped immediately. The authentic packets will be forwarded to next downstream node along the path to the sink node after doing encoding operation. After forwarding, it will store the event_ID and upstream_nodeID in its own cache until it receives ACK_SINK. This process continues up to the sink node. Table III shows the actions taking place in the downstream direction.

5.2.2 Upstream Process. Upstream refers direction towards source node. After veryfing the received packet, the sink node will send an acknowledgement back to the source node through intermediate nodes. The acknowledgemnt, ACK_SINK consists of event_ID and the upstream_nodeID. If a node receives the acknowledgement from sink within the time interval, it will compare the event_ID field in ACK_SINK with the one stored in its own cache. If it matches the corresponding transmission will be considered as successful and removes the corresponidng entry from its own cache and forward ACK_SINK to its upstream node. This process will continue up to the source node. Table IV shows the actions taking place in the downstream direction.

Table 3. BHnFDIA Downstream Process

```
begin
    if (node v == S and S sense some event) then
        msg = append (event_ID, nodeID, type, sensed_data)
        key = DynamicKey(virtual_energy, plaintextID)
        pc = RC4(key, plaintextID)
        msg_pc = encode(msg, pc)
        pkt = append(plaintextID, msg_pc)
        forward pkt to next hop
        wait(t)
        cache(event_ID)
    end if
    if (node v == FN) then
        receive pkt
        key = DynamicKey(virtual_energy, plaintextID)
        pc = RC4(key, plaintextID)
        msgID = decode(pkt, pc)
        x = compare(msgID, plaintextID)
      if (x==true) then
            reencode and forward pkt to next hop
            wait(t)
            cache(event_ID, upstream_nodeID)
       else
            try to find key by decrementing virtual_energy
            threshold times. If failed drop packet.
     end if
    end if
end
```

Table 4. BHnFDIA Upstream Process

```
begin
    if (node v == sink) then
        verify pkt
        send ACK_SINK in upstream direction
    endif
    if (node v == FN) then
        receive ACK_SINK
        if (ACK_SINK event_ID ==cache event_ID) then
            remove corresponding entry from cache
            forward ACK_SINK in upstream direction
        endif
    endif
end
```

5.2.3 Addressing Black Hole Attack. When a packet traverses from source node to sink node through multiple hops, if a malicious node acts as a black hole, it will drop all the incoming packets without forwarding to sink node [4]. So no acknowledgement will be sent to upstream node. After timeout the node just before the attacker in the downstream direction will mark the malicious node and will send a negative acknowledgement, NACK towards the source node. The successive packets received at the node just before the black hole in the downstream direction will be re-directed using another route to the sink node. Also it will broadcasts an ALERT_INFO message to all its neighbours so that they can also avoid this particular node from the routes.

Table 5. Detection and Elimination of Black Hole Attack using BHnFDIA

```
begin
    Let j = 0,threshold=5, SN=Suspected Node
    if (node v == predecessor(SN) in downstream direction) then
        wait for ACK_SINK till time-out
        if time-out occurs
            send NACK towards S
            increment j
            wait for ACK_SINK for next packet
            if j exceeds threshold then
                mark SN as BH
                re-direct successive packets to another route
                broadcast ALERT_INFO among neighbours
            endif
        endif
    endif
end
```

5.2.4 Addressing Communication Errors. When a packet or ACK traverses through the network, they can be lost due to some communication errors. For example, consider Fig 2. If node C fails to receive an ACK_SINK from its downstream node D, it cannot immediately consider the downstream node as malicious. So node C will transmit a threshold number of packets and wait for acknowledgements before considering node D as malicious. Even after transmitting packets threshold times (same or different packets), if node C fails to receive ACK_SINK, the downstream node D will be considered as malicious or black hole. Table V shows black hole detection and elimination (BHnFDIA) algorithm.

5.2.5 Keying process. This process involves dynamic key generation. When a node sense some data, it must authenticate the sensed data before transmitting to sink node. Here virtual energy-based keying process is used [2]. The dynamic key is generated as a function of current virtual energy of the sensor node. The key for first packet is generated as a function of initial virtual energy and initial vector of sensor node. Later keys are generated based on current virtual energy and previous key of sensor. The functional states of sensor node will deplete its virtual energy.

5.2.6 Cryptographic mechanism. In order to avoid excessive use of resources, the cryptographic mechanism should be simple and cost efficient. Here RC4 encryption mechanism is used. The dynamic key obtained from keying process is fed to RC4 algorithm. The resultant permutation code is used to encode the packet to be transmitted which consists of ID, TYPE, DATA and event_ID fields. Along with the encoded packet, plaintext ID of node is also transmitted. The resultant packet format is : $\{$ID, $\{$ ID, TYPE, DATA, event_ID $\}_{pc}$ $\}$.

6. IMPLEMENTATION AND PERFORMANCE EVALUATION

6.1 Simulation Setup

We evaluate the performance of the scheme by simulation and compare it with other schemes in terms of packet delivery rate and filtering efficiency. The simulation was run using $MATLAB$.

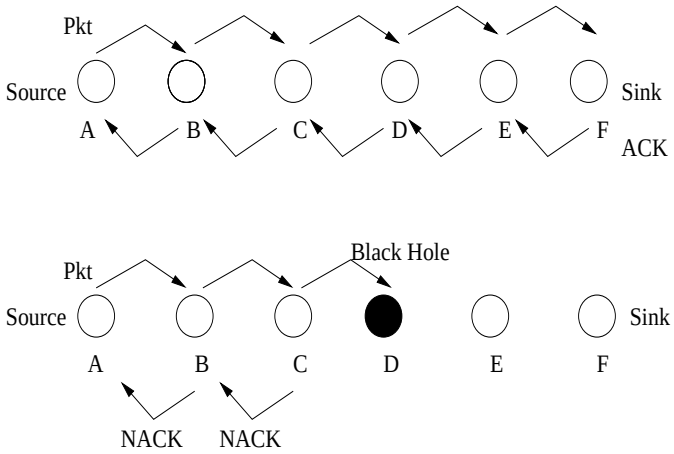

Fig. 2. Transmission without and with Black Hole

Nodes are randomly deployed into $100 \times 100 m^2$. Sink node is located at the downstream end. All sensor nodes are assumed to have same communication ranges. Each node forwards the sensed report to downstream neighbour node until the report reaches the sink node. The sink node forwards the acknowledgement to upstream neighbour node until it reaches the source node. The routing algorithm is deployed on unreliable MAC protocol and there may be ACK or packet drops in the network.

Attackers may inject false data into the network using outside malicious nodes. The network may also experience black holes. Outside attackers may have spoofed valid node identifier. The inside attacker may have all the valid cryptographic details of the node.

6.2 Results and Analysis

6.2.1 Computation Energy. Considering the computation cost required for BHnFDIA is similar in the downstream process of VEBEK. But in the Upstream process each node forwards an ACK packet received from sink to next node till source which increase the computation and communication cost. But with our scheme if a node is identified as a Black hole an ALERT_INFO packet is broadcasted among neighbors and eliminate BLACK HOLE.

6.2.2 Packet Delivery Rate. The packet delivery rate is calculated as the ratio between the number of packets that are sent by the source node and the number of packets that are received by the sink node. Fig 3 shows the results for successful packet delivery rate of our BHnFDIA algorithm without enabling re-transmissions. The x-axis represents the number of compromised nodes or black holes in the network and y-axis represents the packet delivery rate. The simulations are done for varying number of packets.

As can be seen from the figure, packet delivery rate increases with increase in the packet count. This is because only a small threshold number of packets, say 5, need to be dropped in the process of detecting a single black hole. After dropping threshold packets, the upstream node of black hole will re-route the successive packets and inform neighbour nodes to avoid black hole through ALERT_INFO message. The downward slope is obviously due to the increase in black holes. As the number of compromised

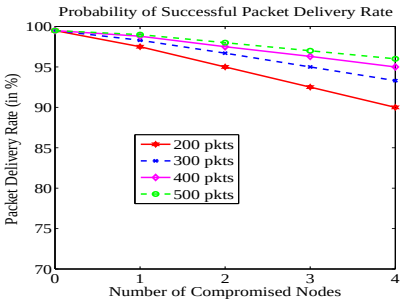

Fig. 3. Successful Delivery of Packets to Sink Node

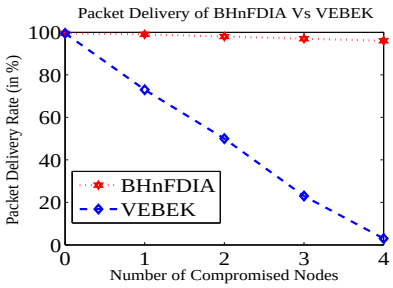

Fig. 4. Comparison of packet delivery rate of BHnFDIA and VEBEK

nodes increases, more packets will be dropped until black holes are detected.

6.2.3 Comparison of Packet Delivery Rate of BHnFDIA and VEBEK. Fig 4 compares the packet delivery rate of BHnFDIA and VEBEK schemes in the presence and absence of black holes. The x-axis represents the number of compromised nodes and y-axis represents the packet delivery rate. When there are no black holes, both schemes have almost same packet delivery rate. But when black holes are present, our scheme has 30%-95% more successful packet delivery. This is because VEBEK has no mechanism to handle insider attacks. But our scheme can overcome black hole attacks leading to higher rate of packet delivery to sink node. Fig 5 shows total energy required as transmission cost of various methods. As BHnFDIA needs ACK cost total energy cost is more compared to VEBEK but with added attack detectection capability. It is better than other previous works as shown in figure.

6.2.4 Filtering Efficiency of BHnFDIA. As authenitcation is performed at every hop, malicious data inserted by outside attackers will be dropped within one hop itself. Hence the filtering efficiency is almost 100%, that is irrespective of the number of malicious packets probability of dropping malicious packets is always within one hop.

7. CONCLUSIONS

Since WSNs are used for several confidential applications, security is a major concern. In this paper, Black Hole detection and Elimination (BHnFDIA) algorithm is proposed to efficiently overcome black hole attacks in WSNs. If some compromised nodes act as

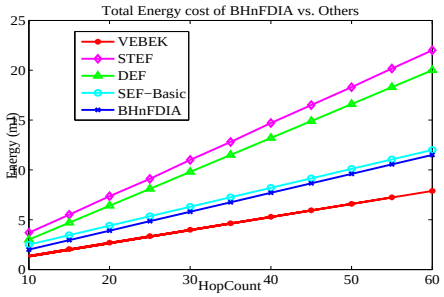

Fig. 5. Total Energy cost of different schemes

black holes then they will drop all the received packets without forwarding to destination sink node. This will intensely affect the packet delivery rate. BHnFDIA provides a new acknowledgement based detection scheme which helps to simplify the elimination of black holes and guarantees successful delivery of packets to destination. Like insider attacks, outside attacks can also threaten the security and energy aspects of sensor nodes by injecting false messages thereby reducing the life time of sensor network. BHnFDIA algorithm can also eliminate false data injection by outside malicious nodes.

Simulation results show that BHnFDIA can successfully overcome black hole and false data injection attacks. Our scheme can successfully identify and eliminate 100% black hole nodes. Since authentication is performed at every hop malicious packets are immediately removed with 100% filtering efficiency. Our scheme ensures more than 99% packet delivery with increased network traffic. Our future work will incorporate other insider attacks without adding much communication overheads.

8. REFERENCES

[1] Tanveer Zia, Albert Zomaya, "Security Issues in Wireless Sensor Networks," *Proc. Intl Conf. Systems and Networks Communication (ICSNC 06),* Oct.2006.

[2] Uluagac A.S, R.A Beyah, Y.Li,J.A.Copeland, "VEBEK : Virtual Energy-Based Encryption and keying for Wireless Sensor Networks," *IEEE Transactions on Mobile Computing,* vol.9, no.7, pp.994-1007, July 2010.

[3] Misra S, Bhattarai K, Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks ," *Proc. International Conf. Communications(ICC 2011),* July 2011.

[4] L.K Bysani, A.K Turuk, "A Survey On Selective Forwarding Attack in Wireless Sensor Networks," *Proc. International Conf. on Devices and Communications (ICDeCom)*, Feb 2011.

[5] Kaplantzis.S, Shilton. A, Mani.N., Sekercioglu.Y.A, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines ," *Proc. Third International Conf. on Intelligent sensors, Sensor Networks and Information* pp 335340, Dec 2007.

[6] Zhen Yu, Yong Guan, "A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks," *IEEE/ACM Transactions on Networking,* vol.18, no.1, pp.150-163, Feb.2010.

[7] H.Hou, C.Corbett, Y.Li, R.Beyah, "Dynamic Energy-based Encoding and Filtering in Sensor Networks," *Proc. IEEE Military Comm. Conf.(MILCOM 07)*, Oct.2007.

[8] Uluagac A.S, R.A Beyah, J.A Copeland, "TIme-Based DynamiC keying and En-Route Filtering (TICK) for Wireless Sensor Networks," *Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2010)*, Dec.2010.

[9] Lin He, Yi-Ying Zhang, Lei Shu, A.V Vasilakos Myong-Soon Park, "Energy-efficient Location-dependent key management Scheme for Wireless Sensor Networks," *Proc. 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010.

[10] M.Ba, I.Niang, B.Gueye, T.Noel, "A Deterministic key Management Scheme for Securing Cluster-based Sensor Networks," *Proc. 2010 IEEE/IFIP Intl Conf. on Embedded and Ubiquitous Computing*, pp.422-427, Dec 2010.

[11] Y.Hu, Y.Lin, Y.Liu, W.Zeng, "RAS:A Robust Authentication Scheme for Filtering False Data in Wireless Sensor Networks," *Proc 15^{th} Intl Conf. on Networks,2007 (ICON 2007)*, pp.200-205,Nov 2007.

[12] C.Braub,M.Schneider, K.Bayarou, C.Eckert, "STEF:A Secure Ticket-Based En-route Filtering Scheme for Wireless Sensor Networks," *Proc. Second Intl Conf. on Availability, Reliability and Security (ARES 07)*, April 2007.

[13] C.Wang,T.Wei, "The Design of an En-route Filtering Mechanism with Immediately Lightweight Authentication for Wireless Sensor Networks," *Proc. 2010 Intl Computer Symposium (ICS)*, pp. 364-369, Dec 2010.

[14] T.Yuan, S.Zhang, Y.Zhong, J.Ma, "KAEF:An En-route Scheme of Filtering False Data in Wirelss Sensor Networks," *Proc. IEEE Intl Conf. on Performance, Computing and Communications,2008 (IPCCC 2008)*, pp.193-200, Dec 2008.

[15] K.Ren, W.Lou, Y.Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol.7, no.5, pp.585-598, May 2008.

[16] B.H Kim, S.Y Moon, H.Y Lee, C.Sun, T.H Cho, "Cluster Adaptation Method to Enhance Performance of Filtering Scheme in Sensor networks," *Proc.11^{th} Intl Conf. on Advanced Communication Technology (ICACT 2009)*, pp. 411-416, Feb 2009.