Chapter 55
Elimination of Black Hole and False Data Injection Attacks in Wireless Sensor Networks

R. Tanuja, M. K. Rekha, S. H. Manjula, K. R. Venugopal, S. S. Iyengar and L. M. Patnaik

Abstract Wireless Sensor Networks (WSNs) are currently being used in a wide range of applications that demand high security requirements. Since sensor network is highly resource constrained, providing security becomes a challenging issue. Attacks must be detected and eliminated from the network as early as possible to enhance the rate of successful transactions. In this paper, we propose to eliminate Black Hole and False Data Injection attacks initiated by the compromised inside nodes and outside malicious nodes respectively using a new acknowledge scheme with low overhead. Simulation results show that our scheme can successfully identify and eliminate 100 % black hole nodes and ensures more than 99 % packet delivery with increased network traffic

Keywords Security · Sink acknowledgement · Negative acknowledgement · Black hole attack · Packet delivery rate

R. Tanuja (✉) · M. K. Rekha · S. H. Manjula · K. R. Venugopal
Department of Computer Science and Engineering,
University Visvesvaraya College of Engineering, Bangalore University, Bangalore,
e-mail: r_tanuja@yahoo.com

S. S. Iyengar
Florida International University, USA

L. M. Patnaik
Indian Institute of Science, Bangalore,

V. V. Das (ed.), *Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing*, Lecture Notes in Electrical Engineering 150,
DOI: 10.1007/978-1-4614-3363-7_55,

55.1 Introduction

In Wireless Sensor Network the 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. 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. This paper proposes to detect and eliminate black hole attack which is a simple form of selective forwarding attack, where a malicious node may drop all the packets passing through it without forwarding to the sink node. We consider false data injection attack from outside malicious nodes i.e. where an attacker injects false data reports into the network and depletes the energy of the forwarding nodes.

55.2 Related Works

Zia and Zomaya [1] have analyzed Attacks, countermeasures and threat models in different layers of WSNs. 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, without any need for specific rekeying messages. 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 in WSNs. 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 developed a centralized Intrusion Detection Scheme (IDS) based on Support Vector Machines and sliding windows. It uses only two features to detect selective forwarding and black hole attacks. Ba et al. [6] have discussed a deterministic key management scheme, DKS-LEACH, to secure LEACH protocol against malicious attacks.

55.3 Problem Definition and Algorithm

Sensor Networks are deployed in harsh, unattended remote areas that are susceptible to various inside compromised node attacks (Black Hole) and outside malicious node attack (False Data Injection attacks). Node based authentication using cryptographic keys is ineffective in addressing insider attacks. The outside

malicious node false data injection attacks needs to be detected and eliminated. The objectives are: (i) To detect and eliminate black hole attack using a new acknowledgement scheme with low overhead. (ii) To ensure authenticity and integrity of transmitted packets by preventing false data injection by outside malicious nodes.

55.3.1 Algorithm

The algorithm for detection and elimination of Black Hole and False Data Injection attack consists of six steps:

(i) Keying process: This process involves dynamic key generation. When a node senses some data, it must authenticate the sensed data before transmitting to the sink node. Here we have used virtual energy-based keying process [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 the sensor. The dynamic key obtained from keying process is fed to RC4 algorithm to get permutation code Pc. The permutation is mapped to a set of actions to be taken on the message. Eg., Simple operations like shift, interleaving, 1's complement etc. The resultant packet format is: {ID, {ID, TYPE, DATA, event ID}Pc}.

(ii) 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 forward the packet along with its plaintextID to next hop and wait for a pre-defined time to receive sink acknowledgement from its downstream neighbor. It stores the event ID in its cache until it receives ACK_ SINK.

(iii) Adressing False Data Injection attacks: When a forwarder node receives a packet, it authenticates the packet by performing virtual energy-based decoding and compares the plaintextID with decodedID. Malicious packets inserted by outsiders (False Data Injection attack) 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 55.1 shows the actions taking place in the downstream direction and elimination of False Data Injection.

(iv) Upstream Process: Upstream refers direction towards source node. After verifying the received packet, the sink node will send an acknowledgement back to the source node through intermediate nodes. The acknowledgement, ACK SINK consists of event ID and the upstream nodeID. If a node receives

Table 55.1 Algorithm for downstream process of BHnFDIA

```
Let t= predefined time, msg_pc=message encrypted using pc, FN=Forwarder
node S=source ;
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)
   endif
   if ( node v == FN) then
       receive pkt
       key = DynamicKey(virtual_energy, plaintextID)
       pc = RC4 (key, plaintextID)
       msgID = decode (msg,pc)
       x = compare(msgID,plaintextID)
       if (x == true) then
          reencode and forward pkt to next hop
          wait(t)
          cache(event_ID,upstream_nodeID)
       else
          find key by decrementing virtual_energy threshold times
          if failed drop packet
       endif
   endif
end
```

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 corresponding entry from its own cache and forwards ACK SINK to its upstream node. This process will continue up to the source node.

(v) Adressing Communication Errors: When a packet or ACK traverses through the network, they can be lost due to some communication error. A node C will transmit a packet threshold number of times and wait for acknowledgements before considering the downstream node D as malicious. If node C fails to receive ACK SINK, the downstream node D is considered as malicious or black hole.

Table 55.2 Algorithm for upstream process of BHnFDIA

```
(i) 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 form cache
            forward ACK_SINK in upstream direction
       endif
   endif
end
(ii) Elimination of BH attack
 Let j = 0, threshold = 5, SN = suspected node
begin
    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
             redirect successive packets to another route
             broadcast ALERT_INFO among neighbours
          endif
       endif
    endif
end
```

(vi) Addressing Black Hole Attack: When a packet traverses from source to sink 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]. No acknowledgement is be sent to upstream node. After timeout, the node just before the attacker in the downstream direction marks the malicious node and sends 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. It will broadcast an ALERT INFO message to all its neighbours so that they can avoid this particular node from the routes. Table 55.2 gives the steps involved in downstream process and elimination of Black Hole attack.

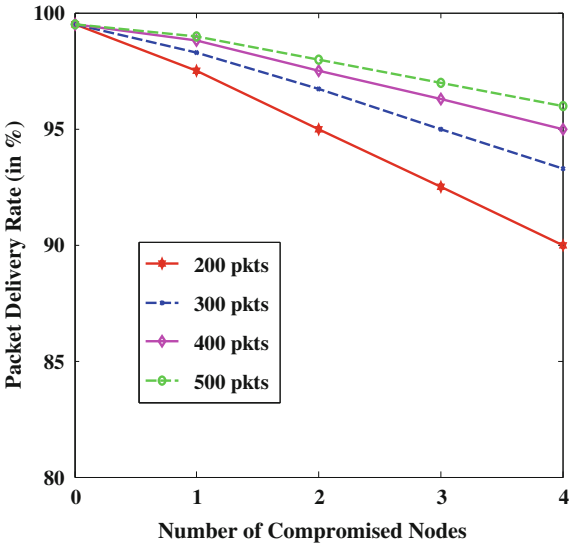

Fig. 55.1 Successful delivery of packets

55.4 Implementation and Performance Evaluation

We evaluate the performance of our scheme by simulation using MATLAB and compare it with other existing schemes in terms of packet delivery rate and filtering efficiency. Nodes are randomly deployed into 100 × 100 m^2. All sensor nodes are assumed to have same communication ranges. The routing algorithm is deployed on unreliable MAC protocol and there may be ACK or packet drops in the network. The network 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.

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. Figure 55.1 shows the results for successful packet delivery rate of our algorithm without enabling re-transmissions. As can be seen from the Fig. 55.1, 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 informs neighbor 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 nodes increase, more packets will be dropped until all the black holes are detected.

Comparison of Packet Delivery Rate: Figure 55.2 compares the packet delivery rate of BHnFDIA with previous work VEBEK schemes in the presence

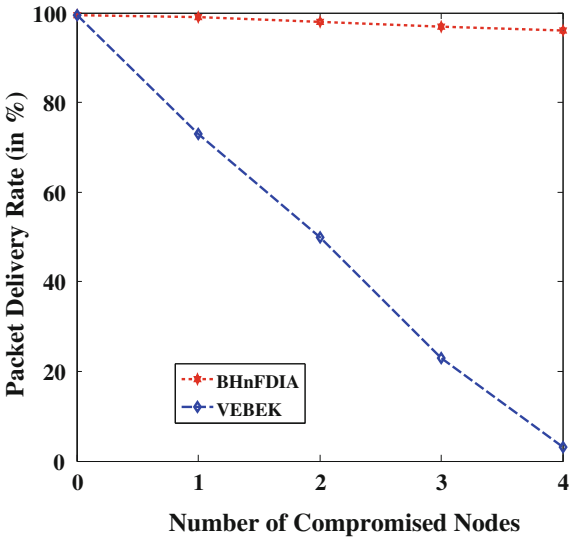

Fig. 55.2 Comparison of packet delivery

and absence of black holes. 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. The energy consumption for keying process being same for both, but with ACK_SINK packet our scheme provides more security to address insider attacks As authentication 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 %, irrespective of the number of malicious packets.

55.5 Conclusions

In WSNs for several applications, security is a major concern. In this paper, we propose algorithm to overcome Black Hole and False Data Injection Attack (BHnFDIA) in WSNs. It provides a new acknowledgement based detection scheme which helps to simplify the elimination of black holes and guarantees successful delivery of packets to destination. Our algorithm can eliminate false data injection by outside malicious nodes. Simulation results show that our algorithm 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.

References

1. Tanveer Z, Albert Z (2006) Security issues in wireless sensor networks. In: Proceedings international conference systems and networks communication (ICSNC 06), Oct 2006
2. Uluagac AS, Beyah RA, Li Y, Copeland JA (2010) VEBEK: virtual energy-based encryption and keying for wireless sensor networks. IEEE T Mobile Comput 9(7):994–1007
3. Misra S, Bhattarai K, Guoliang X (2011) BAMBi: blackhole attacks mitigation with multiple base stations in wireless sensor networks. In: Proceedings international conference communications (ICC 2011), July 2011
4. Bysani LK, Turuk AK (2011) A survey on selective forwarding attack in wireless sensor networks. In: Proceedings international conference on devices and communications (ICDeCom), Feb 2011
5. Kaplantzis S, Shilton A, Mani N, Sekercioglu YA (2007) Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In: Proceedings third international conference on intelligent sensors, sensor networks and information, pp 335–340, Dec 2007
6. Ba M, Niang I, Gueye B, Noel T (2010) A deterministic key management scheme for securing cluster-based sensor networks. In: Proceedings 2010 IEEE/IFIP international conference on embedded and ubiquitous computing, pp 422–427, Dec 2010