THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Time Based Detection and Mitigation of Black Hole At-tack in WSN Using FBPE and MN-ID Algorithm

Neha Bisht
M.Tech. Student, Uttaranchal University, Dehradun, India
Ambika Agarwal
Assistant Professor, Department of Computer Science and Engineering, Uttarakhand University, Dehradun, India

Abstract:
Wireless sensor networks (WSN) define the field of network that consists of small to large number of autonomous Sensing Nodes, which are distributed spatially and possess the sensing, computational and transmission capabilities. Though being very much equipped the Sensing Nodes, also suffer from limitations, the main of them being low power devices, and the problem of data security and data privacy. The nodes being spatially deployed according to the target plan make the network highly vulnerable to internal and external attacks. Hence making security in WSNs a challenge.
A leading DoS attack on WSN is the Black hole attack. In Black hole attack, a malicious node always gives the false replay for any Route request without having specified route to the destination and drops all the received packets. In this paper, we have proposed a three-tier technique to detect and mitigate the Black hole attack. We have proposed TDS a time-period based network intrusion detection technique, which would sense the whole network cluster for any ambiguity and then validating the attack as blackhole attack by FBPE method, and then finally mitigating it by MN_ID method.

Keywords: *Blackhole attack, confirmation agent, frequency, malicious node, time-period, WSN*

1. Introduction

Wireless Sensor Network (WSN) provide a new model for sensing and dispersing information from various environments, aiming to serve numerous and different applications. Due to the continuous advancements, the wireless sensor networks have been recognized as the most fundamental advancement of the century. This is the outcome of the recent advances in electronic sensors, communication technologies and computation algorithms. Wireless sensor networks (WSNs) comprise of an extensive number of autonomous sensing, [1] computing, and communication elements that give a user or administrator the ability to instrument, observe, and react to events and phenomena in a specific environment. The wireless nodes envelop embedded electronic sensors along with battery and RF devices. The purpose of these sensors is to sense and recognize diverse physiological parameters, for instance, temperature, pressure, air pollution etc., to communicate with the neighboring nodes and process the gathered data. Their application space is huge as they can be deployed in various fields like agriculture, smart homes, structures, target tracking, health care, military surveillance and earthquake observation and so on.

In spite of the fact that WSNs are utilized with in numerous provisions, still they pose some limitations [2]. These limitations ought to be looked into while outlining protocols for WSNs. One of the security limitations is the blackhole attack. The blackhole attack is a denial of service attack, where, a malicious node always gives the false Replay message for any Route request without having specified route to the destination and drops all the received packets. The blackhole alters the routing protocols [5] in the cluster so that the sender node would select a path through the malicious node to the destination node.

The blackhole attack can just be visualized as the blackhole occurring in the universe, gulping all things that pass it even not even light can escape it. In this attack, a pernicious node acts as a blackhole to lure all the traffic of the nodes in its vicinity, and does not pass it to other nodes.

A black hole attack is carried by an external adversary [3] on a subset of the sensor nodes in WSN. An adversary captures and re-programs the nodes so that no transmission of data packets occurs from it i.e. it accepts the routing packets but does not forward them to the legitimate neighbors. The blackhole has a tenacious way of attracting the traffic towards itself, the malicious node compromises the routing protocol to advertise that it has the shortest path to the destination node [11,12].

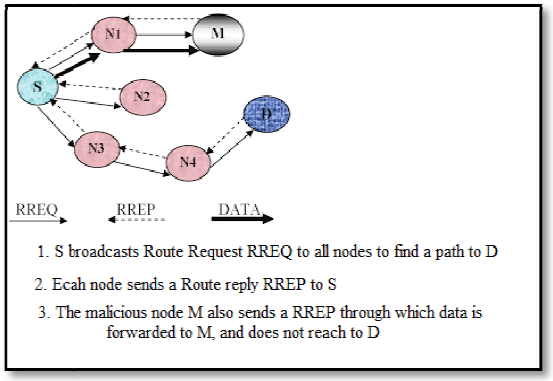

Figure 1: Blackhole Attack

Two types of black hole attack can be distinguished [5].

1.1. Internal Black Hole Attack

This type of black hole attack has an insider malicious node that sits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

1.2. External Black Hole Attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it takes control of internal malicious node and control it to attack other nodes.

Blackhole attacks have serious impact on routing algorithms, [6] which uses sequence numbers to determine fresh messages and select the shortest route based on the hop count such as Dynamic Source Routing (DSR) or Adhoc On-Demand Distance Vector Routing (AODV).

The proposed work proceeds as, in Section II. Us given the Literature Review of some previously done work. In section III is given the proposed work which is divide into three sections. In section IV is the conclusion and in section V is the future work.

2. Related Work

- Yong, Garhan et.al [1] have given a detailed survey article on WSN. They have given the security issues in each network layer for WSNs, the attacks and their countermeasures and their cryptographic solutions, the key management, secure routing and data aggregation, broadcast authentication and, intrusion detection. They have also classified and compared various key management protocols in WSNs.
- Perrig, Stankovic and Wagner [2] have discussed low-level security primitives to high-level security mechanisms, DoS tacks, node resilience, secure routing, Secure data aggregation, Intrusion detection, Secure group management.
- Huisheng Gao, Ruping Wu et.al [3] proposed the identification and prevention of blackhole attack to lessen the likelihood of selecting a blackhole node in the route discovery process. This strategy works successfully for examination and characterizes blackhole assault attack.
- Tseng, Chou and Chao [4] have given an extensive survey on blackhole attacks, from their explanation to their classification, have compared various single blackhole detection schemes and collaborative blackhole attack detection schemes.
- Kamatchi and Mukesh [5] used random dispersive routes reduced delay is achieved even after presence of a blackhole. Energy efficiency is increased with a high rate of security.
- Sarma, Sharma and Das [6] discussed some of the techniques already given to detect and prevent Black hole attack in MANET using AODV protocol and based on their shortcomings have proposed a new methodology to protect against it. peer-to-peer computing, radio-wave propagation, routing protocols, telecommunication security, have also been discussed.
- Mandala, Abdullah et.al [7] have discussed several types of attacks, and then variedly discussed the blackhole attack. Recent efforts for preventing the blackhole attack are discussed. They have categorized the prevention of the blackhole attack into three categories, i.e., Protection based on Cryptography, Protocol Modification, and Intrusion Detection and Counter Measure.
- Mohanapriya and Krishnamurthi [8] have proposed an algorithm that uses destination node to detect the presence of malicious node in the source route and with the help of intrusion detection system the malicious nodes are removed from the network. Their algorithm is very much energy efficient.

3. Proposed Work

The proposed work has been divided into 3 main steps, so that there can be intrusion detection, malicious node recognition and the mitigation against black hole attack.

3.1. Network Intrusion Detection

The WSN is always sub divided into clusters so that the communication between sensors is both manageable and rapid. Detection of intrusion can be done by determining which cluster in a network has been compromised the detection can either come out positive and negative. If the detection comes positive, then we can take a step further in our work to determine the compromised node.

Here we are proposing a Time period based Detection Scheme [TDS]. This is on a timely basis checks the cluster for intrusion. The scheme can be explained as:

a. Select a time period [tp] for which a cluster remains operative. When t < tp, where t is the system time, then the algorithm checks for a compromised node and after (tp) is over the algorithm would run again.
b. Each sensor node in the cluster sends the data packet (DP) which contains address of the respective cluster member node ($CM_{adr)}$, the packets received via which node ($Rec_{CMi \rightarrow CMj}$) and the packets forwarded to which node (For $_{CMj \rightarrow CMk}$)

DP [($CM_{adr)}$, ($Rec_{CMi \rightarrow CMj}$), (For $_{CMj \rightarrow CMk}$)]

c. When the sensor node gets all the packets from the cluster members, the sensor compares the respective info with it routing table

$[S_{RT}] \cong [CM_{DP}]$

Where $[S_{RT}]$ is the information of Sender Routing Table and $[CM_{DP}]$ is the Cluster Member Data Packet.

d. After comparing it can be determined that which node is accepting packets and is not forwarding packets, then except the Destination node the node would be our malicious node.

Tmp_{CM} is a temporary node which has been determined as Malicious (M) and D is the destination.

3.1.1. Time Period Detection Scheme (TDS) Algorithm

```
if  (tp < T)
  then
  {
    Send [[(CM_adr), (Rec_CMi →CMj), (For CMj→CMk)]
to sender.
      Compare [S_RT] with [CM_DP]

   if  (Tmp_CM is same as D)
   then
    No intrusion
   else
     {
      Intrusion Detected
      Determine Tmp_CM as M
      Run FBPE
      }
    }
else
Start Over
```

Table 1: TDS Algorithm

3.2. Malicious Node Confirmation

Even if in the above algorithm a cluster member is termed as a malicious, but a confirmation is required, as a node can be dead or damaged. Hence confirmation is necessary.

From the previous algorithm the address of compromised node has been noted as M_{adr}.

In the confirmation the sender request a route to D through M_{adr} intentionally and checks the frequency of discarded packets. If the frequency of discarded is more than that of received then the malicious node is confirmed.

3.2.1. Frequency Based Packet Exclusion (FBPE) Algorithm

```
Send RREQ from S to D via M
Send RREP from M
Send Confirmation Agent (CA) from S to
visit M
CA checks freq
if (freq drop > freq send)
      then
        {
         list M as Blackhole
        }
     else
     {
       list M as damaged node
     }
```

Table 2: FBPE Algorithm

3.3. Mitigation of Blackhole Attack MN-ID Algorithm

```
S broadcasts M adr in cluster
Select shortest path S→D
Drop all RREP outgoing from M
Assign MN-ID to all CM in SP
if  (MN-ID = IMN-ID)
   {
   Send data packet to IMN
   }
else
  {
  Drop IMN and run FBPE for IMN
  }
```

Table 3: MN-ID Algorithm

Where MN-ID is member node in a shortest path for a cluster.
IMN-ID is the intermediate member node id for the shortest path in cluster.
CM is Cluster member and SP is Shortest Path.

4. Conclusion

WSN is a cutting edge network framework for almost all sensor networks. Its application ranges from military applications, to communication, weather forecasting, to healthcare. But the formulators have to be aware of the various attacks on this network, and in the above mentioned work we had proposed a novel range of algorithms to sense, confirm and mitigate the blackhole attack.

5. Future Work

In future, we can have extended the proposed work for being energy efficient, lessen the acknowledgement messages sent, and performance effective.

6. References

i. Akyildiz,W.Su, Y.Sankarasubramaniam, and E.Cayirci,(2002). Wireless sensor networks: a survey. Computer Networks, 38.
ii. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences,1(4), 1-16.
iii. Adrian Perrig, John Stankovic, David Wagner (2004). Security in wireless sensor networks. Communications Of The ACM , 47(6), 53-57.
iv. HuishengGao,Ruping Wu,Mingjing Cao, Can Zhang(2014). Detection and Defense Technology of Blackhole Attacks in Wireless Sensor Network. Algorithms and Architectures for Parallel Processing, 601-610.
v. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(4), 1-16.
vi. HuishengGao,Ruping Wu,Mingjing Cao, Can Zhang(2014). Detection and Defense Technology of Blackhole Attacks in Wireless Sensor Network. Algorithms and Architectures for Parallel Processing, 601-610.

vii. V. Kamatchi , Rajeswari Mukesh, Rajakumar (2012). Securing Data from Black Hole Attack Using AODV Routing for Mobile Ad Hoc Networks. Advances in Computing and Information Technology, 177.365-373

viii. K.J.Sarma, R.Sharma and R.Das(2014). A survey of Black hole attack detection in Manet.Issues and Challenges in Intelligent Computing Techniques (ICICT),202-205.

ix. S. Mandala, A. H. Abdullah, A. S. Ismail, H. Haron, M. A. Ngadi and Y. Coulibaly (2013. A review of blackhole attack in mobile adhoc network. Instrumentation, Communications, Information

x. Technology, and Biomedical Engineering (ICICI-BME), 339-344.

xi. M.Mohanapriya,IlangoKrishnamurthi (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers and Electrical Engineering archive, 40(2),530-538

xii. B.R.Baviskar, V.N.Patil (2014). Blackhole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms. International Journal of Advent Research in Computer & Electronics, 2(1).

xiii. Wazir Zada Khana, Yang Xiangb, Mohammed Y Aalsalema, Quratulain Arshada (2012). The Selective Forwarding Attack in Sensor Networks: Detections and Counter measures. I.J. Wireless and Microwave Technologies, 2, 33-44.

xiv. S.Sharma and R. Gupta, (2012). Simulation study of black hole attack in the mobile ad-hoc networks. journal of engineering science and technology, vol. 4, no. 2 pp. 243-250.

xv. H.Weerasinge and H.Fu ―Preventing Black Hole Attack in Mobile Ad hoc Networks: simulation, implementation and evaluation. international journal of software engg. and its applications,vol2,no3 in MANET, Journal Of Networks, Vol. 3, NO.5.

xvi. Jian Yin, Sanjay Madria, A Hierarchical Secure Routing Protocol against Black Hole. IEEE SUTC 2012 Taiwan, 5-7 June 2012.

xvii. AtulYadav et al., ―Study of Network Layer Attacks and Counter measures in Wireless Sensor Network. International Journal of Computer Science and Network (IJCSN) Volume 1,Issue 4, August 2012.

xviii. Dokurer, S.; Ert, Y.M.; and Acar, C.E.(2011). Performance analysis of ad hoc networks under black hole attacks. SoutheastCon, proceeding IEEE 148-153.

xix. Dr. Karim Konate and Abdourahime Gaye(2011),,a proposal mechanism against the attacks: cooperative black hole, blackmail, overflow and selfish in routing protocol of mobile ad hoc network. International journal.

xx. Satyajayant Misra, Kabi Bhattarai, and GuoliangXue ―BAMBi: BlackholeAttacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings.

xxi. Gulshan Kumar, Mritunjay Rai and Gang-soo Lee ―Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement. International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012.