International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

RESEARCH ARTICLE

ISSN: 2321-7758

DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

N.GEETHA PRIYA[1], A. JAYA KUMAR[2]
[1]UG student,[2]Associate professor
Department of ECE, IFET College of engineering, Villupuram, Tamil Nadu, India

N.GEETHA PRIYA

A. JAYA KUMAR

ABSTRACT
Wireless sensor network has a self autonomous environment which communicates over wireless links. Wireless sensor networks have an additional problem of security because nodes are often placed in a unfriendly or dangerous environment where they are not actually sheltered, hence they are lying face down to many kinds of attacks and one of them is black hole attack. In this attack a malicious node falsely claiming it to have the new and direct path to the destination and drops all the receiving packets. In this project we projected an approach for better study and improve security using monitoring node and knowledge table. The monitoring node frequently verify the knowledge if it detect any packet loss it analysis the reason for packet loss and reconstruct the path using this the packet loss ratio can be reduced and the attacker can be found and removed from the transmission.

Keywords: WSN, Blackhole attack, Routing protocol, monitoring node, knowledge table

INTRODUCTION

Wireless sensor networks have become a growing area of research and development due to tremendous amount of application which provide benefits for such system and leads to the development of tiny, cheap, and self contained battery powered computers known as sensor nodes. The wireless sensor network is compiled with large number of sensor nodes, these nodes are used to interact with their environment to sense and to control the physical parameters, these nodes have to collaborate to fulfill their tasks as, usually as a single node is incapable of doing so; and they use wireless communication to enable this collaboration hence it also contain some computation, wireless communication, and sensing or control functionality.

These networks will also include actuators and the term wireless sensor network has become the commonly accepted name. Sometimes, other names used are wireless sensor and also actuator networks where frequently used.

The sensor nodes have limited storage capacity and are deployed in harsh environment and in difficult locations, the radio transmitter are implemented to transfer the collected data to base station.WSN have many applications such as military target tracking surveillance, disaster relief, health monitoring, seismic sensing, environment exploration, and to measure the environment.

In this project we have introduced an additional node called as monitoring node this node used to verify the data transmission frequently a knowledge table is used to verify this transmission. It contains data about forwarded and received packets which is used to determine the problem for data loss and also helps to verify the solution to stop the data loss.

BLACK HOLE ATTACK

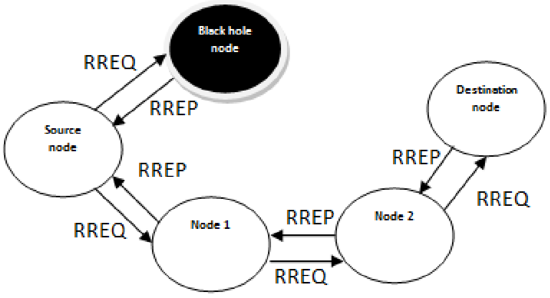

Fig.1. Black hole attack

Blackhole is one of the serious attacks in which attacker node advertises itself as having a good route to the destination and tries to attract traffic towards itself. Once a source node receives the route advertised by attacker node, it selects the same route for data transmission and starts sending data packets. When attacker node receives traffic from source, it drops all of received packets which it had to forward further. Due to this, packet delivery ratio gets decreased and all resources utilization is wasted.

In AODV protocol, first phase of data transmission is Route Discovery. Route detection starts by broadcasting a Route Request (RREQ) packet by source node. On receiving RREQ packet, each node checks its cache for an existing route to the destination. If there exists a route, intermediate node unicasts a Route Reply (RREP) packet to source node else, RREQ is further forwarded to neighbor nodes. Source decides route's freshness by using Destination Sequence number in RREP packet. Higher the Dest_Seq number, fresher the route would be. When a malicious node receives an RREQ packet, it replies to source node by unicasting a forged RREP.

This RREP contains a higher valued Dest_Seq number, due to which source assumes it is a fresh and valid route to destination and starts transmission on that route. At last, Black hole node receives data packets from source and intentionally drops them. Initially source node broadcasts a RREQ packet. When it reaches to Black hole node, it generates an RREP with higher Dest_Seq number and unicasts it to source. Source on receiving a RREP starts transmission which leads to packet drop by Black hole node.

RELATED WORKS

Routing protocols which aims to find secure route based on Public Key Infrastructure (PKI), where network has to depend on third party and also,PKI adds extra overhead regarding key maintenance. The protocols aim to mitigate black hole attack taking in account packet drop but not considering the reasons for packet drop. In this paper we present a novel approach to mitigate black hole attack while considering packet drop reasons.

Fidel Thachil et al. in[2]proposed a method to mitigate black hole attack in which each node monitors its neighbor by maintaining a cache which records the packets forwarded to the neighboring nodes. The node checks the packet it forwarded to its neighbor is being further forwarded or not and based on it a trust value is calculated on the neighboring node. If the trust value of a node goes below a predefined threshold, it is declared malicious. The paper calculates trust value based on packet drop but does not consider packet drop reasons.

L TamilSelvan et al. in [3] proposed a solution which modifies AODV such that it stores more than one RREP. In 'TimerExpiredTable' a timer is set after receiving first RREP. All the replies that arrived before the timer expires are stored in 'Collect Route Reply Table' (CRRT). All received RREP are checked by source for repeated next hop node to destination, after timer is expired. An RREP is chosen if it is repeated next hop, else a random RREP is chosen. In case there is no repeated node, it's difficult to predict maliciousness.

Satoshi Kurosawal. in [4] gave an anomaly detection scheme in which more than one RREP is received by source nodes after RREQ broadcast. The average of difference between Dest_Seq in RREP packet and the one in the list is calculated as threshold by source node. This threshold is used to detect malicious node. This Dest_Seq number can be learnt by the malicious node, which can make a relatively large Dest_Seq number making it difficult to detect.

Sukla Banerjee [5] proposed an approach in which destination is notified about communication through a prelude message sent by source. Meanwhile flow of data is monitored by neighboring nodes. Postlude message which contains number of packets received is sent by destination which is helpful in deciding data loss rate to the source node. Malicious nodes detection and removal is initiated by the response collected from network and monitoring nodes. Due to additional packet routing mechanism has increased routing overhead.

Payal N. Raj et al. in [6] proposed DPR AODV in which method from [5] is used to calculate threshold value, which helps in deciding node's honesty. To prevent further attack on finding a malicious node an ALARM message is sent to all nodes in the network. In the beginning of transmission malicious node detection is not possible as calculated threshold has to be used next time and also ALARM packets increase routing overhead.

Ankita V. Rachh et al. in [7] proposed an approach called EBAODV (Enhance Black hole AODV), which creates leader nodes for detecting malicious nodes. A timer is set as the source node generates RREQ. Before expired time if RREQ is received a fake packet is sent to destination and on receiving acknowledgement (ACK) original packet is sent by source. Packets are dropped if ACK is not received. Method for selection of leader nodes is not given. Sending fake packets causes additional overhead and packet drop reasons are not considered.

Sanjay Ramaswamy et al. [8] have proposed a method in which, every node maintains a table called Data Routing Information (DRI). DRI table contains three fields node_id, from and through. Value for from and through are in 1 (true) and 0 (false). Source Node (SN) broadcasts RREQ to all, then intermediate node (IN) replies to SN with RREP along with its Next Hop Node (NHN) information and its own DRI. After that SN checks its own DRI to confirm whether RREP sender is reliable or not. If it is reliable, SN starts transmission else, SN sends Further Request (FRq) to NHN of RREP sender. NHN will reply using FRp to SN. SN based on reply (FRp) decides the reliability and either starts transmission or broadcasts malicious list accordingly. Extra FRq and FRp from neighbor add overhead in processing.

Vishnu K. et al. [9] proposed a mechanism to detect and remove the black and grayhole attack. This mechanism makes use of Backbone Nodes (BBNs). BBNs are used to provide Restricted IP (RIP). Source initially requests nearest BBN to allocate an RIP. After getting RIP, source broadcasts RREQ for RIP as well as destination. If source receives RREP for only destination, it means no malicious node is there. Else, a notification message is sent to all nodes by source node and source transmits dummy packets to destination. Every node monitors data flow in network and if data loss exceeds normal threshold then the neighbor nodes broadcast alert message through the whole network, and add the malicious nodes to the black hole list so that, in future all replies from malicious node will be dropped. This mechanism adds control overhead by broadcasting RREQ for RIP and maintaining RIP at BBNs.

Ming-Yang et al. [10] introduced an Intrusion Detection System called Anti-Blackhole Mechanism (ABM). Each IDS executes ABM. Abnormal difference between RREQs and RREPs transmitted from the node are used to calculate suspicious value of that node. When suspicious value goes beyond threshold a block message is broadcast by nearby IDS. Three assumptions are made to use this method, two neighbor IDS should be within each other's transmission range, an authentication mechanism to prevent block message and node id forging. Authentication mechanism adds overhead in processing.

Jhaveri R.H et al. [11] have given a method in which a PEAK [7] value is calculated for every time interval. It is maximum possible Dest_Seq value at that instance. If an intermediate node replies with Dest_Seq number higher than PEAK, it is marked as DO_NOT_CONSIDER in same RREP. Then routing table is modified by detector node. Same RREP is forwarded to source. Source on receiving RREP, generates a malicious list and broadcasts it along with RREQ. Every node in network updates their routing table entries for detected malicious node and node gets isolated from network. PEAK value calculation requires additional processing.

Thachil et al. [12] proposed an approach where, every node monitors neighboring nodes. Depending on number of packet forwarded to and from a node, its trust value is calculated by its neighbor node. If Trust value is less than threshold, range value is decreased and if it is greater than threshold, range value is incremented. If range value goes below threshold, node is identified as malicious node. Detecting node, broadcast a message in network to notify all others about presence of malicious node so as to avoid future transmission through it. Trust table maintenance adds additional overhead to processing.

AODV PROTOCOL

The protocol (AODV) Ad Hoc On-demand Distance Vector Routing is a reactive unicast routing protocol for mobile ad hoc networks. The AODV used to operates in two phases such as route discovery and route maintenance AODV uses route discovery by broadcasting route request message to all its neighboring nodes, and the Sequence numbers will helps in avoiding the process of distributing the same packet more than once.

When a source node requires a route to a destination, it broadcasts a route request message across the network. These broadcasted route request message is received by each node which is present in the network during its travel each node increases the hop count by one. If an route request message with the same route request ID is received, the intermediate node which present in the network will simply rejects the newly received RREQs.

An RREQ arrives at a node will create a current route to the destination node. If an intermediate node in the network has a path entry for the desired destination, it used to determine whether the path is shortest path which will compare the sequence number in the routing table of destination node in its own routing table to the destination sequence number in the RREQ. If the route requests sequence number for the destination node is greater than that recorded by the intermediate node, then the intermediate node should not use the recorded route to respond to the route request. Instead the intermediate node will again broadcasts the RREQ message when the destination or intermediate node discovers a fresh enough route to the destination node by receiving the RREQ message which create an route reply message and update their routing tables with register the hop count and the sequence number of the destination node.

Afterwards the route reply message is unicasted by a destination node to the source node by broadcasting a route request from source node and, the Route can be maintained by means of route error (RERR) packets. RERR (Route Error) is initiated by the intermediate node if there is any path failure. It will propagate to all the affected destinations. The route error will lists all the nodes affected by the link failure. When the intermediate node detects a path failure (via a link-layer feedback), it generates a route error message. The RERR(route error) propagates towards all traffic sources having a route via the failed link, and remove all broken routes on the way of data transmission.

A source node upon receiving the RERR initiates a new route discovery by again re transmitting the route request message. Apart from this path maintenance system, AODV also has a timer-based mechanism to purge stale routes.

In AODV protocol, the routing table contains the Following fields:

<(DI)destination IP address,
destination sequence number,
next-hop IP address,
hop-count,
entry expiration time>

PROPOSED SYSTEM

a. Secure knowledge algoritm: In the proposed system we have modified the performance of existing system by including separate monitoring node and additional performance has been included in the knowledge table. We have also modified that in promiscuous node every node monitors the data being transferred by its neighbor node, and transfer the details of packet transmission to monitoring node. This monitoring node has all information about the node in the path of data transmission; it has all details of knowledge table.

The shortest paths are initiated by the source node, it broadcast route request (RREQ) message to all nearby nodes the route request contains address of destination node. Every node has a routing table which has the IP address of recently transmitted packets. Hence the intermediate node verify the route request address with the routing table if the address match then intermediate node transfer the route reply (RREP) message to the source node in this way the shortest path is determined. The above data's are stored in every node and also in monitoring node.

The monitoring node consists of knowledge table which has all the details of packet transmission. With previous knowledge table [1] we have additionally included trusted node, with this trusted field we can easily identify the malicious node. The monitoring node frequently verify knowledge table when the data loss reaches the threshold level then the monitoring node check the reason for packet loss. If the loss is due to less power the monitoring node just transfer the path to another nearby node, but if the loss is due to malicious node then whole path is reconstructed. This is the new function included in this project.

b. Algorithm:

Notations:-
SN: Source Node
DN: Destination Node
IN: Intermediate Node
RT: Routing Table
MN: Malicious node
NN: Neighbor of malicious node
PM: Promiscuous mode
MALNOT: Malicious Notification

```
{
SN broadcasts RREQ
IN receives RREQ
if (IN.RT has Route to DN)
Send RREP to SN;
else
Forward RREQ to Neighbor nodes;
Shortest path is found;
Data stored in monitoring node;
Starts transmission;
while(fm < threshold)
{
if(Current node is NN)
{
increment fm;
if(in PM received Packet From MN)
increment rm;
}
if(rm = 0)
Broadcast MALNOT;
Reconstruct path;
}
```

c.Notification mechanism: When Blackhole node is identified, Neighbor Node takes initiative to notify all nodes in the network and it broadcasts a packet called MALNOT. The given figure shows format of MALNOT packet.

Trusted node id	Malicious detector id	Malicious id	Destination id	Life time	Time stamp

Fig.2. MALNOT packet format

This packet contains fields like Packet type, malicious detector id, malicious id, Destination id, Lifetime and Time Stamp. Packet type is used to distinguish this packet from data and control packets. Malicious detector id is used for Neighbor Node detecting malicious node. Malicious id is used for Blackhole node. Lifetime and Time stamp for packet lifetime and packet generation time respectively.

d. Knowledge table:

fm	**rm**
Packet transferred from source to intermediate node	Packet transferred from intermediate node to destination node

fm maintains recent packet received

rm maintain information about recent packet transferred

This knowledge table used to identify whether the output is received by destination are not. The forwarded and received message details are stored in the monitoring node when the received message is not equal to the forwarded message then the node used to reconstruct the shortest path again.

RESULT AND DISCRIPTION

For simulation, we used network simulator NS2. We took two simulation scenarios. In first scenario, we varied number of packet loss and in the second scenario network life time. Every source node was allowed to transmit 350 packets, each packet with a size of 520 bytes. Threshold for *fm* was 30. In first scenario, we randomly increased the packet delivery ratio by reducing the loss of packet during data transmission. There was above 80% of packets are delivered without any loss or attack using AODV protocol. The loss of packet will be in 5 to 8% where in existing system it is above 15%.

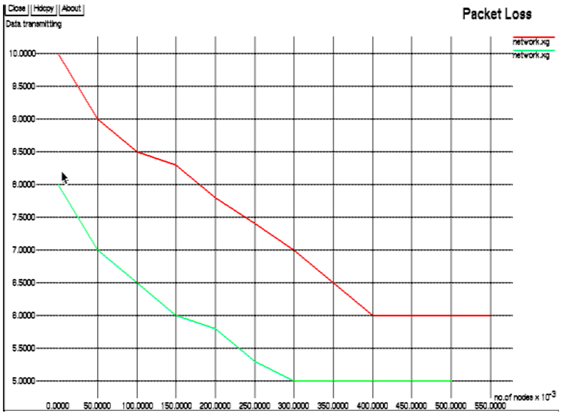

Fig.3. Packet loss ratio in proposed system

The next scenario explained in fig 4, which describes about the network life time. To increase the life time of network the power consumption of ever node must be less. The packet loss ratio will also increase in case of low battery level and the efficiency of the node reduced due to this condition in order to avoid this we need to increase the network life time.

We use the help of Network Simulator Version-2 (NS2) to simulate our proposed model. We have successfully implemented secure knowledge algorithm to secure AODV routing protocol against black hole attack using NS- 2.35. This method gives better performance compared to existing AODV protocol in throughput & Delay. The main objective of simulation is to prove proposed method is properly securing existing AODV with all security aspects in terms of black hole attack.

Total number of nodes	ten, twenty, thirty
Medium access control	802.11
Simulator	NS2-2.34
Simulation time	250s
Routing Protocol	AODV
Transmission range	200m
Node Speed	10 - 80 m/s
Traffic model	CBR

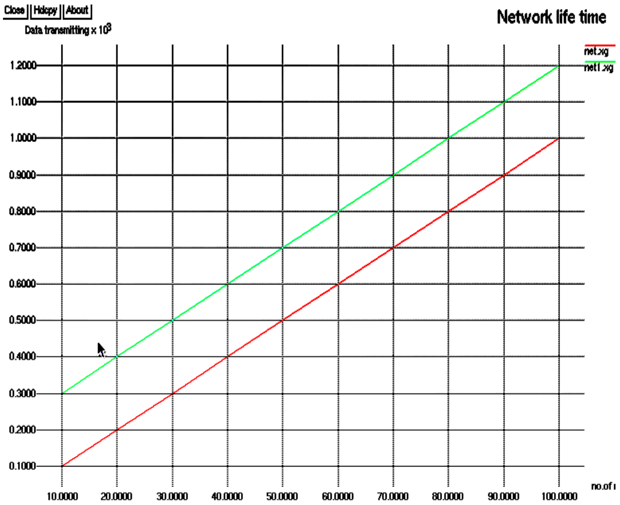

Fig.4.Network life time

CONCLUTION

In this approach, we simulated detection and prevention of black hole attack by using secure knowledge algorithm.

Detecting the malicious node using the knowledge table and by using the monitoring node is useful and it also helps to provide low data loss with high amount of efficiency. The network life time has been increased above 80% due to this system and the packet loss ratio is also above 85%. This amount is also capable to withstand during cooperative black hole attack. Using this algorithm the cooperative black hole can also be detected and eliminated.

REFERENCE

[1]. AyeshaSiddiqua, KotariSridevi, Arshad AhmedKhan Mohammed, “Preventing black hole attacks in MANETs using secure knowledge algorithm” spaces-2015 dept of ece, K L university

[2]. Fidel Thachil, K.C. Shet, "A Trust Based Approach for AODV protocol to Mitigate Black hole attack in MANET," 2012 International conference in Computing Science.,IEEE 2012.

[3]. TamilSelvan, L.; Sankaranarayanan, V., "Prevention of Black hole Attack in

MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21,21, 27-30 Aug. 2007.

[4]. Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." In: International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007.

[5]. Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", World Congress on Engineering and Computer Science, October 2008, pp. 337-342.

[6]. Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet." In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.

[7]. Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit, "A Novel Approach for Detection of Blackhole Attacks "IOSR Journal of Computer Engineering (IOSR-JCE) e- ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74

[8]. Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative blackhole attack in wireless Ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[9]. Vishnu K, Amos J Paul "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks" In: International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 22, 2010

[10]. Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on , vol., no., pp.162,167, 6-9 Sept. 2010

[11]. Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C., "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad Hoc Networks," Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on , vol., no., pp.556,560, 7-8 Jan. 2012

[12]. Thachil, F.; Shet, K. C., "A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET," Computing Sciences (ICCS), 2012 International Conference on , vol., no., pp.281,285, 14-15 Sept. 2012 IEEE – 31661 4th ICCCNT 2013 July 4

[13]. A.Rajaram, Dr.S. Palaniswami,"Malicious Node Detection System for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol.1 (2), 2010.

[14]. Y.-C. Hu, D. B. Johnson, and A. Perrig, "Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," The 4th IEEE Wksp. Mobile Computing Systems and Applications (WMCSA'02), June 2002

[15]. C. Castelluccia and G. Montenegro, "Protecting AODV Against Impersonation Attacks," ACM SIGMOBILE Mobile Comp. and Commune. Rev. Archive, vol. 6, no. 3, July 2002.

[16]. A. Jayakumar, " Study Analysis of Cross QOS based Scheduler for 3.9G LTE Network" International Journal of Scientific and Engineering Research(IJSER), Volume4, Issue7, July 2013(ISSN 2229-5518)

A Brief Bio of Authors

N.Geethapriya[1] is currently pursuing her bachelor degree in IFET College of engineering in 2016 and as she had interest in wireless sensor network so she had engaged in this work. This work helps to detect and prevent Blackhole attack using monitoring node and the knowledge table which compare the forwarding packets, using this security of WSN system will be improved.

A.Jayakumar[2] received his B.E degree from Sun College of engineering and technology in 2003 and M.E degree from noorul islam college of engineering in 2006 and he is currently working as associate professor in IFET college of engineering. He had decade of experience in teaching and he is a fellow member of the ISTE. His research interest lies in the field of wireless communication, digital signals and signal processing. He had reached some international journals such as International Journal of Scientific and Engineering Research (IJSER), International Journal of Trend in Research and Development, and some international conference.