IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 3, Issue 5, Oct -Nov, 2015
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Energy Efficient Intrusion Detection System for Black Hole Attacks

Akshay Sabale
Pimpri Chichwad College of Engineering, Savitribai Phule Pune University,
Pune, Maharashtra,411044, India

Abstract
Wireless sensor networks (WSN) are severely susceptible to attack. Black hole is one of the most malicious attacks. Black hole attacks target sensors routing protocols. This kind of attacks can have bad impact on hierarchical routing protocols. Numerous security solutions have been recommended to secure WSNs from malicious attacks (black hole attacks). But, most of these solutions are complex in nature and are energy inefficient. In this paper, I propose an ordered energy proficient intrusion recognition system, to protect Wireless sensor network from black hole attacks. Paper is based on exchange of control packets between sensor node and base station. A malicious node can be cluster head, and absorbs all received data from its cluster members. For detecting Black hole attacks, we use energy efficient Intrusion Detection System and LEACH protocol.

Keywords: *Black hole attack, HSRBH Protocol, Wireless sensors network, Cluster head (CH).*

1. Introduction

Security is the principal obstacle of many applications in the wireless sensor network (WSN). Security protocols are designed for powerful machines, and are not suitable for Wireless sensor networks. Routing data is an important task, and must be secured from malicious attacks. Hierarchical protocols are most efficient for routing data. However they are extremely susceptible to routing attacks. In hierarchical WSNs network is typically organized into clusters. It means organized with cluster heads (CHs). CHs are responsible for tasks such as collecting and processing data, and forwarding the results towards the base station (BS). Attacks involving CHs are particularly damaging, because CHs are responsible for critical functions.

One of the most damaging attacks is the black hole attack .it target cluster heads. A cluster head can be selected as malicious node, and absorbs all received data from its cluster members. It attracts the entire traffic to be routed through it by telling itself as the shortest route. Thus, the attacker received message by rejecting and not forwarding it. Selective forwarding is a type of black hole attack. Instead rejecting all received packets, adversary node or selects random that will be rejected.

To detect black hole attacks, each wireless sensor node must send periodically to the Base Station, the number of packets sent to its CH. A second cluster head is selected to forward control packets to the Base Station. Black hole table is maintained by each sensor node to prevent the selection of malicious nodes as cluster heads.
he text must be in English. Authors whose English language is not their own are certainly requested to have their manuscripts checked (or co-authored) by an English native speaker, for linguistic correctness before submission and in its final version, if changes had been made to the initial version. The submitted typeset scripts of each contribution must be in their final form and of good appearance because they will be printed directly. The document you are reading is written in the format that should be used in your paper.

This document is set in 10-point Times New Roman. If absolutely necessary, we suggest the use of condensed line spacing rather than smaller point sizes. Some technical formatting software print mathematical formulas in italic type, with subscripts and superscripts in a slightly smaller font size. This is acceptable.

2. Literature survey

In this paper, black hole attack detection system in cluster based communication is discussed. To detect a black hole attack, author makes nodes that monitor their neighbourhood and then communicate between each other to decide if there is an intrusion taking place. The scheme is further evaluated on a real Wireless Sensor Network. This scheme benefits from the neighbours monitoring so that there is a kind of distribution that will minimize the load on a detection node. There will be an increase in the communication messages between nodes during the

collaboration and as a result will deplete the power of nodes quickly.

A hierarchical secure routing protocol called HSRBH, was developed to detect and find a secure path from source node to destination node against black hole attacks. To find a safe route against black hole attacks, HSRBH uses only symmetric key cryptography. Most of black hole attacks except the group leader should do agreement with other nodes to make black hole attack. So it is much quicker in discovering the black hole attacks, and the communication is very low. The developed protocol also offers the system to identify the black hole attack caused by the group leader agreement with other nodes. However, the solution is not scalable due to high computation processes and communication overhead. Another security solution was developed, where sensor node performs power control to transmit a packet to more than one SNs, in the direction of the BS. In the case if any node that is on the forwarding path does not forward a packet, this event will be identified by its next hop neighbour on the forwarding path and will report the BS as a black hole attack. This scheme is very costly for a network with z black hole nodes, for each original message, O(z) extra messages are essential, which is very expensive.

Author developed the use of multiple base stations for improving data delivery in the presence of black hole attacks. However, multiple base stations bring extra overhead and increase the communication and memory cost.

Detecting Black hole attack leads to secured transfer of packet over the wireless sensor network. It avoids the damage of whole network and also leakage of information

3. Proposed intrusion detection scheme

3.1 Tables and Figures

Detecting black hole attack in WSNs is given below

1] Cluster member wants to send the data to base station over WSNs so it transmits to selected nearest cluster head and similarly this cluster head again send data to next selected cluster head. In this way cluster heads to another cluster head transmits that data towards base station for send it to other cluster. Finally, data packet reaches to the destination.

2] Cluster member can also send data directly towards base station but it not possible because energy of CH is inefficient for sending data packet directly to base station

3] Selection of cluster head is most important process in sending data packet to destination. One cluster head not able to send data packet due to energy is not sufficient. For that purpose, CH select the second cluster head for transmit data packet. It is helpful to translate data fast to the base station.

4] CH send the packet. packet contain two field one is identifier and another one is number of data received from cluster head. Selection of second cluster head is very simple, whose energy reserve capacity is more this node should be selected as SCH. Similarly, third cluster head is selected in same way.

5]Packet received at base station then. Nbrpk that is number of packet send from cluster head is compared with packet received at base station for detecting black hole attack.

6] If number is not match then base station alarm broadcast an alarm packet to all network nodes alarm contain identifier of black hole attacker. In this way Black hole attack is detected, with the help of identifier we detect black hole attacker node. Identifier of the node is attached when data packet travels over the particular node to base station. With the help of identifier, we easily detect the black hole attacker node.

4. Conclusions

I studied an intrusion detection system, to secure sensor network nodes from black hole attacks using energy efficient algorithm to prevent attacks on wireless sensor network. I don't firmly tell that the studied mechanism can detect definitively all attacks, but this proposal protects black hole attack in WSN.

Acknowledgments

The author thanks Mrs. Rohini Pise for discussing various possibilities of black hole attack. The author thanks Mrs. Prajktta Vidhate, Ms. Poonam Sabale help in discussing black hole attack.

References

[1] Samir Athmani,. "Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs, no 1-5, 2013.

[2] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro Sensor Networks," IEEE Transactions on the wireless communications, Vol. 1, No 4, pp. 660-670, 2002.

[3] M. Satyajayant, B. Kabi, and X. Guoliang, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE ICC proceedings, 2011.

[4] D. Boubiche, and A. Bilami, "HEEP (Hybrid Energy Efficiency Protocol) Based on Chain Clustering," Int. J. Sensor Networks, Volume 10 Issue 1/2, pp. 25 - 35, 2011.