Scientific Journal Impact Factor (SJIF): 3.518

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Catching BlackHole Attacks in Wireless Sensor Networks

Ashish M[1] and Mr. Jason Martis[2]

[1] *M. Tech, Department Of ISE, NMAM Institute of Technology, Nitte*

[2] *Asst. Prof, Department Of ISE, NMAM Institute of Technology, Nitte*

Abstract- Wireless sensor networks contain multiple nodes, which communicates with each other using a wireless channel. Some of the important applications of WSN include military and Monitoring system. Most of the applications are mission-critical. Due to these facts, providing security is very crucial for these networks. However, providing security for these Networks is usually very complicated due to the fact that, nodes have limited resources. Most of the existing researches are focused on consumption of energy rather than proving security. This paper proposes a method to tackle one of the main security attack, called BlackHole attack.

Keywords- Wireless Sensor Networks, BlackHole attack, Energy efficiency, security in WSN, Packet dropping attack

I. INTRODUCTION

Wireless Sensor Networks (WSN) have nodes with the sensing capability, which are distributed spatially. These nodes first senses any events of interest, then they process it using their limited processing power and finally produce data and communicates with other nodes. Usually there will be a multiple nodes, whose size is very small. These nodes can be deployed in short span of time. WSN technology was mainly developed because of countermeasures for warfare in remote regions. The application of WSN are spreading to various domains in recent years including Consumer applications. During the design process of the WSN, it is important to consider the factors like energy consumption, Reliability, Simplicity and security.

II. LITERATURE SURVEY

Most of the existing methods are based on techniques like authentication or monitoring their neighbouring nodes continuously. In Authentication technique, certificates are most commonly used [2]. In this method, each node will send a unique ID to all the nodes which are within its transmission range. Nodes from which it will get the acknowledgement are considered as neighbouring nodes. This method is very effective in preventing a bad node from entering the network, but it may be not as effective if the bad node is already inside the network. And also, the usage of acknowledgement means, it will have a very high communication overhead. The next technique is based on monitoring the neighbour nodes continuously [8]. In this method, every node will have a watchdog. The watchdog will continuously monitor the neighbouring nodes. After sending every packet, it will check whether the next hop neighbours are forwarding those packets or simply dropping it. This method requires a high amount of energy supply, which makes it not so efficient in Wireless Sensor Networks with limited resources. Fan Ye, Haiyun Luo, Songwu Lu, [3] have proposed a method called Statistical En-Route Filtering of Injected False Data in Sensor Networks which will detect the false responses on the packet forwarding phase. There will be a number of keys, which will be assigned to nodes by using suitable algorithm. If a node wants to send some packets to the sink, the neighboring nodes must add the keys to it before forwarding the packet, which are assigned earlier in the process. So if the added key is invalid, then that means nodes are compromised, and hence it must be dropped. This method only prevents a modified packet from reaching the destination, but it will not identify the compromised nodes. This paper proposes a method which detects the nodes which indulges in the BlackBole attack, with a very high bad node detection ratio.

III. ARCHITECTURE OF THE PROPOSED SYSTEM

WSN are very easy to deploy compared to other traditional systems, and since the nodes are usually physically unguarded, security of WSN is a real concern. The proposed system here overcomes the security attacks like BlackHole attack. BlackHole attack is a denial of service attack, where sensor node which is expected to forward a packet, chooses not to forward it. Attackers can insert malicious codes into the unguarded node's software, so that it will drop the packet. And in addition, in order to avoid being detected, the nodes will drop only few of the packets. Sometimes nodes may modify the original packets before forwarding, so that destination node receives incorrect information. In some of the applications like health monitoring, these are considered very dangerous.

The proposed method shows how the attacks like packet dropping can be detected by flooding mechanism and by using algorithms like node categorization algorithms. Initially, the topology will be established by sink, which floods a packet in entire network. Then the sink maintains tables to check the behaviour of the node, and then by using algorithms like node categorization algorithms, which helps to identify the packet droppers. This system explains a method to identify the nodes which indulges in black hole attacks WSN. The figure shows the architecture of the system.

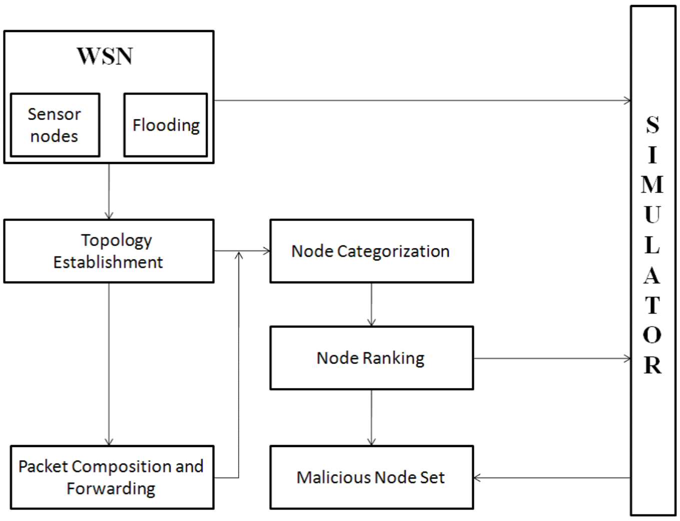

Figure 1: The Proposed system

IV. DECOMPOSITION DESCRIPTION

In this system, Sink will initially establish the topology by flooding the beacon packets. After this, a secret key and a unique ID will be shared between the nodes and the sink. Then the nodes will organize the packets they want to send, and forward it to the other nodes. These upstream nodes will trim few bits from the rear end, and then includes its unique ID and sends it to the next node. The process will go on till packet reaches the destination. Then the Sink will run the node categorization algorithm, after that, finally the node ranking algorithms are run. Few tables are maintained by the sink, which helps to analyse the topology of the system and detect the suspicious nodes. One of them is Path table. After receiving the packets, the Sink will decode them and tracks the node where it was originated and also, information about nodes which forwarded it. These information are entered into a path table. The will contain same number of entries as the number of nodes.

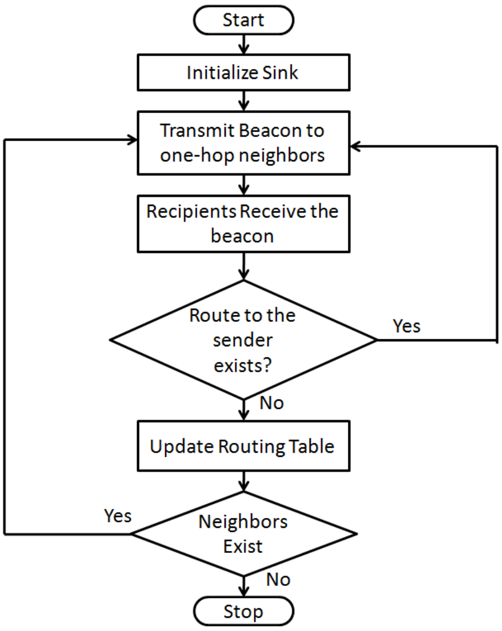
Start
Initialize Sink
Transmit Beacon to one-hop neighbors
Recipients Receive the beacon
Route to the sender exists?
Yes
No
Update Routing Table
Yes
Neighbors Exist
No
Stop

Figure 2: Topology Establishment

In the initialization phase, Simulated WSN nodes will be fed with basic information, which are used to know network and its behaviour. Every nodes will be fed with a random number (RN), which is given to all nodes. RN will be of the same length. The Sink maintains a table to store every RN. This acts like an ID of the node. The presence of RN, which is added to all the packets, guarantees that a compromised node cannot identify the origin of the packet.

The Topology Establishment phase, Deals with the Sink flooding the network with beacon packets. So every nodes receive the beacon packets, and creates the route to the Sink accordingly. The Sink will send beacon at the very beginning of each rounds. Beacon is a packet which contains, the information like Source, and hop count. This beacon is flooded on entire network. Sink sends the beacon to all the nodes which are within its range of transmission. The receiving nodes will create the route to the Sink accordingly.

The Packet Composition phase deals with composing each packet, if a node has any info that it wants to forward to the Sink. One of the most important features of the proposed method is, it guarantees that all packets are of exact same length. This can be done by two types of bit padding. Bit padding means addition of one or more extra bits to make it to a standard size.

Packet Sending and Forwarding phase deals with the some mechanisms for forwarding the composed packets to the Sink securely. This mechanism requires encryption techniques using a secret key that have been loaded into every nodes during the initialization phase. By adding encryption, it adds extra security to the transmission, and also guarantees no modification can be done by attacking nodes.

Packet Reception phase mainly deals with the processing that the Sink required to do while it receives a packet. Each packets adds it ID to the packet it is forwarding. The Sink analyses every bits of each of the packet and then it fills the path table accordingly.

The final phase is called Node Categorization. Here The Sink will run some algorithm for fixed interval of time. The categorization is done using “Dropping Ratio". A threshold value is set by the system, and this value cannot be zero, because few packets may be dropped during collision and other similar events. After this threshold value for goodness ratio is calculated, then we find out goodness ratio of every single node. This can be done by the Sink maintaining many tables. This node categorization algorithms are run for each entry in the path table. The nodes which has low threshold values will be considered as suspicious nodes. All the suspicious nodes will be added to a separate table and by running few algorithms, the nodes which are actually indulges in the BlackHole attacks can be separated from the suspicious nodes.

V. SIMULATIONS AND RESULTS

This method is done using NS 2.35 on a Linux Ubuntu operating system. Topology details are given as input using a .TCL file. Coding is done using C++ language. The files .cc and .h are compiled together, which produces a .o file.

Topology is 250m*250m. And a total of 100 nodes are used. These nodes are distributed randomly inside the network. The sink node can be placed anywhere inside the network, but it has been placed at the centre here.

Now we check how the system performs and produces outputs for different combinations of the bad nodes.

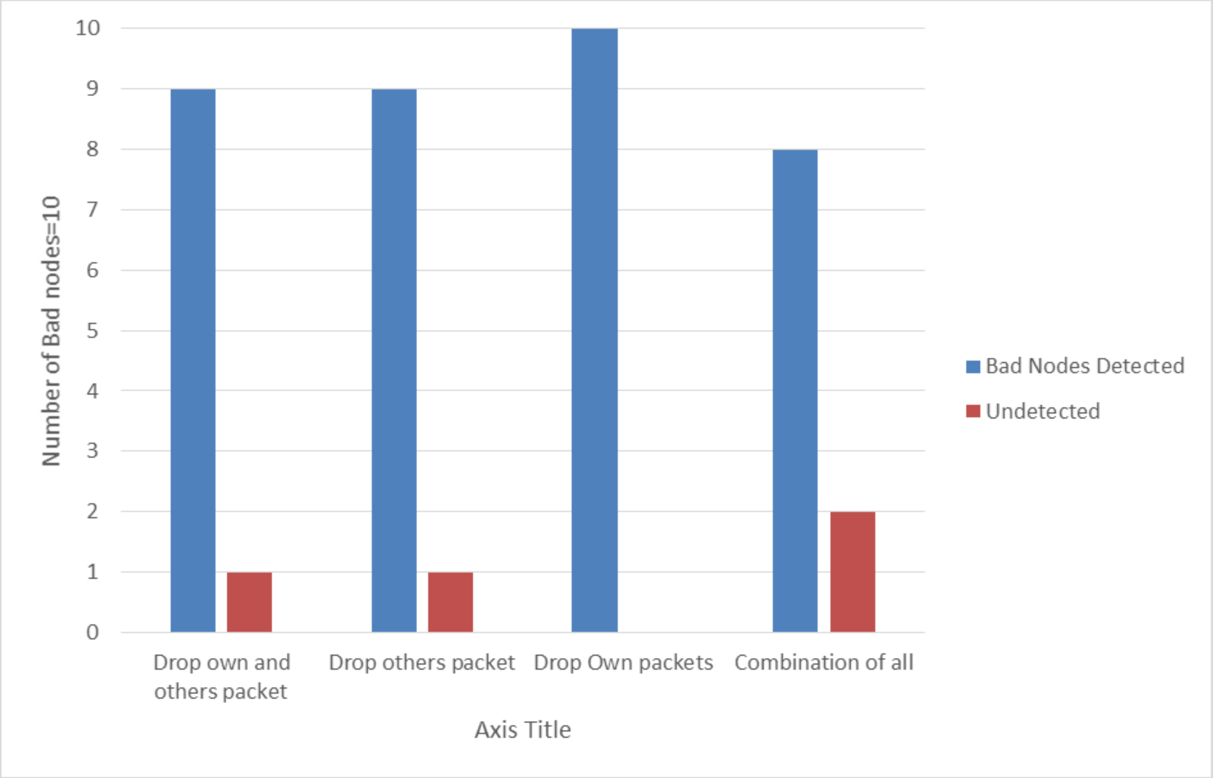

Figure 3: Bad node detection ratio

We consider various scenarios where different number of bad nodes are inserted into the network and each time it acts differently. The bad nodes may be dropping only its own packets, or it may be dropping only other nodes' packets or it may be combination of these two. As shown in the above figure, we use 10 bad nodes for this test case, and these bad nodes drop 33% of the total packets. As we can see, the system was able to find 9, 9, 10 and 8 bad nodes out of 10 respectively, for different types of bad nodes. And also, out of four cases, it never accused any nodes falsely of being a bad node, except for once in the last type of test case.

VI. CONCLUSION

The discussed method is very efficient to prevent the BlackHole attack in WSN. In normal cases, the malicious node will drop every packet it is supposed to forward, which is easy to identify. But this method can detect even those nodes which drops only few packets. Due to the unique packet format we are using in the method, it can overcome the problem of selective dropping. the proposed method has a very good malicious node detection ratio, and a very low communication overhead and also the chances of nodes are falsely being identified as droppers is very low.

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim Guiling Wang, ”Catching Packet Droppers and Modifiers in Wireless Sensor Networks", Vol. 23, No. 5, May 2012,pp.835-843.

[2] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, “A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007

[3] F. Ye, H. Yang, and Z. Liu, “Catching Moles in Sensor Networks," Proc. 27th Int'l Conf. Distributed Computing Systems (ICDCS '07), 2007.

[4] Ms. B.R.Baviskar, Mr.V.N.Patil. \"Black hole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms", International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, April 2014 E-ISSN: 2348-5523

[5] Rupinder Kaur and Parminder Singh, “REVIEW OF BLACK HOLE AND GREY HOLE ATTACK", the International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014

[6] Hao Yang et al., “Security in mobile ad hoc networks: challenges and solutions”, IEEE Wireless Communications, Volume 11, Issue 1.

[7] T. Clausen, P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, RFC 3626, Oct. 2008.

[8] Marti, T. Giuli, K. Lai, and M. Baker, \Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, 2000.