A REVIEW PAPER ON WATCHDOG MECHANISM IN WIRELESS SENSOR NETWORK TO ELIMINATE FALSE MALICIOUS NODE DETECTION

Jijeesh Baburajan[1], Jignesh Prajapati[2]

[1] *Research Scholar, CSE Department, Parul Institute of Technology, Gujarat, India*
[2] *Assistant Professor, CSE Department, Parul Institute of Technology, Gujarat, India*

Abstract

Wireless Sensor network (WSN) are broadly used today in various fields such as environmental control, surveillance task, object tracking, military applications etc. As WSN is an ad-hoc network which is deployed in such an environment which is physically insecure, intrusion detection has been one of the major area of research in WSN. Inorder to achieve an appropriate level of security in WSNs we cannot depend on cryptographic techniques as these techniques fall prey to insider attacks. This paper discusses on watchdog mechanism, one of the intrusion detection techniques in Wireless Sensor Network. Watchdog is a monitoring technique which detects the misbehaving nodes in the network. The main area of focus in this paper is being made to the problems in existing watchdog technique for malicious node detection.

***Index Terms**: Wireless Sensor Network, Security Intrusion Detection, Watchdog.*

----------***----------

1. INTRODUCTION

A wireless sensor network is an ad-hoc network which consists of large number of small inexpensive devices which are known as nodes (motes)[8]. These nodes are battery-operated devices capable of communicating with each other without relying on any fixed infrastructure. The wireless sensor networks (WSNs) are often deployed in such an environment which is physically insecure and we can hardly prevent attackers from the physical access to these devices.WSN consists of base station along with number of nodes that sense the environment and send data to the base station. The base station (sink) is more powerful than other nodes in terms of energy consumption and other parameters and serves as an interface to the outer world. When any node needs to send a message to the base station that is outside of its radio range, it sends it through internal nodes. The internal nodes deployed in WSNs are the same as others, but besides of local sensing they also provide forwarding service for other nodes.

Inorder to achieve an appropriate level of security in WSNs we cannot depend on cryptographic techniques as these techniques fall prey to insider attacks. So to counter this threat some additional measures need to be taken such as an intrusion detection system. Intrusion Detection system tries to detect any kind of intrusions made into the system or network and gives an alert for the malicious event occurred[2]. There are three basic approaches in intrusion detection system according to the used detection techniques which can be classified as, Misuse Detection, Anomaly Detection and Specification Based Detection. First approach (Misuse Detection) compares the observed behavior of the nodes with known attack patterns i.e. signature based. It can measure instances of attacks accurately and effectively but it lacks the ability to detect any unknown attack. Anomaly detection is based on monitoring the changes in the behavior of nodes rather than searching for some known attack signatures. The main disadvantage of this system is the high false positive rates of the nodes being identified. The third approach is similar to anomaly detection but the normal behavior is specified manually as a system of constraints.

The rest of the paper is organized as follows: Section II discusses about major security threats and attack against WSN. In Section III we discuss about the Watchdog mechanism and their limitations in detecting malicious nodes. Section IV discusses the review of strategy been implied to overcome the limitations in watchdog. In Section V we conclude the paper based on the literature review

2. MAJOR SECURITY THREATS AND ATTACK IN WSN

In this section we will discuss about the security attacks in WSN and also the measures taken to counter these attacks[1].

A. Denial of Service (DOS) attacks

DOS attacks can be defined as any kind of activity that can cause adverse effect in a network or even destroy the network intentionally. The main aim of DOS attacks is to overload the hardware of sensor nodes significantly as the hardware of the nodes are usually constrained. Other DOS attacks that are very destructive are jamming and tampering attacks[1].

B. Sinkhole/Blackhole attacks

In this attack, a malicious node acts as a blackhole[1] to pull in all the traffic in the network. When a route request is made for the packets to be delivered to another node, the attacker listens to the request and returns a reply to the intended node that it has the shortest path to the base station. As a result a malicious node acts between the base station and the sensor node

C. Node Replication attacks

In this type of attack, the attacker tries to add a node into the network which use same cryptographic secrets similar to another legitimate node present in the network. The major consequence of this attack is that the data may get corrupted or may cause disruption of some nodes at some parts of the network.

D. Hello Flood attacks

Many routing protocols need to broadcast HELLO packets in order to discover one-hop neighbors. This attack uses such packets as a weapon to attract sensor nodes. In particular, an attacker with a large radio range and enough processing power can send HELLO packets to a large number of sensor nodes by flooding an entire section of the network[1].

E. Wormhole attacks

In this attack, an attacker records the packets at one location in the network and tunnels those to another location with the help of a long-range wireless channel or an optical link[1].

F. Sybil attacks

One of the useful application of WSN is that, for numerous task to be accomplished sensor nodes are required to cooperate with other nodes which then implements management policies to allocate subtasks to different nodes. In this particular attack, an attacked node pretends to be more than a single node by use of identities of other legitimate nodes, restricting the cooperation between nodes. This attack can disrupt the routing mechanisms as well as the data aggregation process.

3. WATCHDOG MECHANISM

The watchdog mechanism[3] is one of the intrusion detection techniques in Wireless Sensor Network. Watchdog is a monitoring technique[3] which detects the misbehaving nodes in the network. As shown in figure1 consider a node A which wants to send a message to node C which is not in its radio range. As a result of which it sends the message

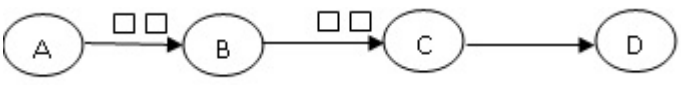

Figure 1 Packet transmission between nodes

through an intermediate node B. When the node B receives a packet from A it then forwards it to C. Here we may consider S_A be a set of nodes which hear messages sent from A to B and S_B be a set of nodes that hear message from B to C. In this way we may define a set of possible watchdogs of the node B as an intersection of S_A and S_B. This means that any node that lies in the intersection region is able to hear both messages and is able to decide whether node B forwards message from node A. This approach relies on the broadcast nature of wireless communications and the assumption that sensors are usually densely deployed[1]. When a message is broadcasted in a network the packet is not only received by the intended node but it is also received by the neighboring nodes within that range. Normally such nodes should discard the packet, but this can be used for intrusion detection. Hence, a node can activate the IDS agent and monitor the packets that are sent by its neighbors by overhearing them.

3.1 Limitations In Watchdog For Malicious Node Detection.

In this section we will describe some the limitations in Watchdog mechanism for detection of malicious node in the network. The Watchdog mechanism has certain limitations[4] because of which it is not able to detect the misbehaving nodes in the network. These are Ambiguous collision, Receiver collision, Limited transmission power, false misbehavior and partial droping.

1. Ambiguous collision: Consider a node A wants to send a packet to node C (see fig.1). Here as C is not within the range of A, the node A sends the packet through node B. Now node A overhears node B whether it is forwarding the packet to the intended node C. It may happen that A does not overhear this transmission at an instance where other neighbor of A sends the packet to it at the same time. This may cause A to conclude that B is malicious, but the node B being malicious may not be true.

2. Receiver collision: Suppose that the node B transmits the packet to node C and also node A overhears the transmission of this packet from B, but it may happen that collision occurs at node C due to some attacks and as a result of which the packet is not received by C.

3. Limited transmission power: If node B can somehow adjust the transmission power in such a way that node A can overhear the transmission from B to C, but C does not receive the packet, then B can drop the packets and may falsely report that it has forwarded the packet to C.

4. False misbehavior: A malicious node intentionally reports that other nodes are misbehaving. Node A can report that B is dropping packets although it is not the case. As a result there may be a neighbor node of A which cannot communicate directly with B, can consider node B as malicious node.

5. Partial dropping: In order to show that node B's failure tally does not exceed the detection threshold of A's watchdog it may drop some packets rather than dropping all the packets

4. STRATEGIES APPLIED TO OVERCOME LIMITATIONS OF WATCHDOG.

In 2012, A. Forootaninia and M. B. Ghaznavi-Ghoushchi[5] a new technique based on watchdog mechanism which is modified and improved by enhancing the security in wireless sensor network. In this proposed algorithm, cluster heads are assumed to be the first layer watchdogs. Here the cluster node consist of a buffer which accommodates all the packets sent by the nodes within in sensing range. All the messages that are send to other nodes is stored first into this buffer. Thereafter at each forwarding of packets the messages are compared with the messages in the buffer. If the messages are similar, the first message in the buffer will be deleted, otherwise it will turn out that the node B has not sent the message or replaced it with another one. The implementation result shows that the improved watchdog has less error than the original watchdog technique and it seems to be more efficient[5]. The proposed algorithm solved the following known problems in watchdog: impartial removal, False Malicious node, limited power transfer and node conspiracy. Table1 shown below describes the problems that have been resolved in the proposed modified watchdog technique[5].

Table -1: Comparison with existing Watchdog

Problems in Watchdog	Proposed watchdog[5]
Creating ambiguous Collision	unsolved
Creating Collision in the receiver	unsolved
selecting the incorrect malicious node	solved
Limited power transfer	solved
Node conspiracy	solved
Impartial removal	solved

In ref[6], Souvik Sen proposed an approach for collision detection in WSN. In the proposed algorithm the author CSMA/CN technique used for collision detection. In CSMA/CN, the transmitter uses one interface for transmitting and the other (correlator) for listening. The receiver uses its single interface for multiplexing between transmission and reception. Transmission is initiated as in IEEE 802.11, except one difference: for every packet, the PHY layer preamble is concatenated with an additional bit sequence, a signature, uniquely computed from the intended receiver's identifier. The transmitter T ensures the channel is idle and transmits this packet using the transmit antenna. The listening antenna, by virtue of being very close to the transmitting antenna, receives this signal with a high signal strength – we call this the self-signal. The packet's intended receiver also receives the transmitted signal and starts decoding the arriving bits. Simultaneously, R triggers collision detection. The drawback of this method is that the collision detection at the receiver is partially avoided. This technique being used in Watchdog still does not avoid the ambiguous collisions.

In ref[7] ,M. Kiran kumar proposed an algorithm for detecting malicious packet dropping due to different kind of security attacks such as blackhole, greyhole and warmhole attacks. In this approach the algorithm detects whether a neighbor node is maliciously dropping packets or not. Initially a node A that sends the packet will count the RTS messages it sent to node B during some interval of time along with the CTS messages received from node B. Then the probability of each node forwarding a packet correctly to another node is evaluated. According to goal defined for Node A to detect any malicious dropping of packet an approximate value of Node A forwarding the packets correctly is calculated. Finally Node A calculates the percentage of packets that is maliciously dropped. If that value is greater than some threshold value then the node is noted as malicious node and it will simultaneously inform the neighbors and may remove the node from routing to other nodes. The simulation results described that less the packet interval time, more will be the load and the probability of collision will be high

5. CONCLUSION AND FUTURE WORK

From the review above papers it can be said that intrusion detection system being an important part in wireless sensor network, we need to have an efficient IDS to counter the attacks made by the intruder. Watchdog technique described above have been used since long, and due to certain limitations it has not been considered as an effective mechanism for malicious detection of nodes. As seen from ref[5], certain problems existing in watchdog has been resolved but still one of the problems in watchdog i.e the malicious node detection due to ambiguous collision of packets has not been solved.

Thus in future, we can extend the proposed work of A. Forootaninia and M. B. Ghaznavi-Ghoushchi[5] to resolve the ambiguous collision of packets in watchdog mechanism.

REFERENCES

[1] Abror Abduvaliyev, Al-Sakib Khan Pathan, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks" in IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013

[2] CE. Loo, MY. Ng, C. Leckie, and M. Palaniswami, Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, vol. 2, pp. 313-332, 2006.

[3] Sergio Marti, T. J. Giuli, Kevin Lai, "Mitigating routing misbehavior in mobile adhoc networks" in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255–265, New York, NY, USA, 2000. ACM.

[4] A.Babu Karuppiah, T.Meenakshi, "False Misbehaviour Elimination In Watchdog Monitoring System Using Change Point In A Wireless Sensor Network" in International Journal of Graduate Research in Engineering and Technology (GRET),2012.

[5] A. Forootaninia and M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks" International Journal of Network Security & Its Applications (IJNSA), 2012 .

[6] Souvik Sen Naveen Santhapuri "Moving Away from Collision Avoidance: Towards Collision Detection in Wireless Networks" IEEE transactions on vehicular technology, vol. 60, no. 2,

[7] M. Kiran kumar, A. Sai Harish, "A Novel Schema for Detecting Malicious Packet Losses" in International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.5, Sep-Oct. 2012 pp-3633-3636

[8] Bc. Lumír Honus," Design, implementation and simulation of intrusion detection system for wireless sensor networks", Brno, spring 2009.

BIOGRAPHIES

Jijeesh Baburajan is currently pursuing Master of Engineering in Computer Science and Engineering from Parul Institute of Technology, Waghodia, Vadodara, India.

Jignesh Prajapati is currently working as an Assistant Professor in CSE dept, Parul Institute of Technology, Waghodia, Vadodara, India