A NOVEL APPROACH TOWARD SECURING ZIGBEE WIRELESS NETWORKS FROM BLACK HOLE ATTACK

SEYYED MOHAMMAD SEDIGH ZIABARI
Department of Computer Engineering, Islamic Azad University, Science and Research Branch, Alborz, Iran

ABSTRACT

As wireless networks has grown rapidly in recent years, the application of network technology is faced with new threats. In this paper, we will try to present a total view of ZigBee protocol which is a useful specification of IEEE 802.15.4 standard, then we will investigate black hole attack toward ZigBee sensor network which uses AODV technique. Finally we will try to present a new security mechanism which will secure ZigBee networks against this attack. With the aid of demonstrated comparison chart-obtained via the implementation of this attack in NS2 software-between a standard ZigBee network and the Secure ZigBee network (the new approach) the improvement and optimality of our novel approach will obviously be comprehendible.

KEYWORDS: ZigBee network; ZigBee protocol; sensor networks; black hole attack; AODV

ZigBee technology provides a secure reliable communication, independent to physical communicational media such as wire (FRANKEL, ET AL., 2007). it also provides a low rate, low consumption communication with the aid of DSSS and Dual physical layer mode (CHEN, ET AL.2012). The rate of power consumption in these networks are so low, that is approximately it equals the shelf battery life (HO & GAO, 2013). it also uses CSMA-CA (MEYER, 2012).

Wireless ZigBee networks support star, peer to peer and mesh networking topologies. It also contains a hybrid topology which consists of a combination between the two latter topologies (CAO, ET AL., 2008). Moreover a reliable communication is guaranteed by using a handshake data exchange protocol (CHIN, ET AL., 2012).

Devices operating in these networks are divided to two categories: FFD and RFD (AYOUB, ET AL., 2011). Coordinator and network routers must be FFD. FFDs use the most energy resources but they have the ability to perform all of the operations such as routing. However, RFDs are used as end devices and their functionality has been reduced (BARONTI, ET AL., 2007).

RELATED WORKS

Considering various advantages of wireless ZigBee networks and including highly secure mechanisms, these networks are known to be totally reliable. Attacks on ZigBee networks can be divided to two categories. Active and Passive attacks. During a passive attack such as Eavesdropping attack, attacker tries to collect key data. On the other hand, during an active attack, such as Packet in Packet attack (BISWAS, ET AL., 2012) and Identity-Based attack (CHEN, ET AL., 2010), attacker tries to penetrate the network and alter data. However, black hole attack which is a sub-branch of Denial of Service attacks (RAMESH, ET AL., 2012) can cause great damages to ZigBee networks. In the following part, first we try to introduce this type of security attacks and then try to avoid it, using our novel approach.

From a holistic view, black hole attack is considered a DoS attacks in which attacker would try to introduce itself as an authorized and valid node among other nodes. It then commences to receive the packets from a sender node and this have the ability to launch many security threats such as Eavesdropping (AMEEN, ET AL., 2010), key sniffing (YUKSEL, ET AL., 2012), altering packet and then resend it to the intended receiver or basically dropping all of the received packets, which is the case of our research and novel approach.

As mentioned above, during a black hole attack, the assailant creates a node and introduces it to the other network nodes as a neighbor node. This means that whenever a node tries to send a packet to its destination, the black hole node with the declaration of a low hop count or high signal feasibility during routing protocol operation, will try to catch the packet and then drop it (Wazid, ET AL., 2013). When this happens, the sender would not receive any acknowledgment messages, so it resends the packet after a timeout operation. With the repetition of this procedure, the damages toward the sensor node (SINGHAL, ET AL., 2012) for discussed
network would be colossal. From one aspect with the increase in dropped packets in network, the lifetime of packets would be reduced. Moreover, resending packets over and over again will heighten network’s data traffic and will diminish network’s throughput.

PROPOSED METHOD

As mentioned before, ZigBee specification mainly operated on network layer (Ahmed, 2005-2009). thus, attacks on network layer can be of great importance.

There have been some researches about a secure routing protocol in ZigBee networks. One the more effective techniques is AOMDV (Wazid, ET AL., 2013) which uses multipath clustering distance vector to form clusters and divide the network into several clusters, in which there lies a cluster head (Bhatia & Kaushik, 2008).

After considering different approaches toward this attack we used two main features of this security threat against it. The first feature of black hole node is the declaration of low hop count (Wazid, ET AL.2013). In order to receive the packets the black hole node will set a climax of two hop counts. The second feature is the non-acknowledgment nature of this menace. In our novel approach first we try to detect the black hole node then would try to eliminate it from authorized network nodes list. In the following section we will present our new algorithm.

1) During the routing protocol we consider the nodes with the highest hop count of two, as suspicious nodes. You should keep in mind that in this stage we would not claim, nodes with the maximum number of two hop count are black holes. Considering the scale of the network, there may be some valid nodes with the hop count of one or two. But in the next stage we will clarify the situation.

2) In this stage, a test packet is built. This is actually a dummy packet and the content of the packet is of no concern to us. We just want to realize whether the suspicious nodes which the test packets are sent to them, will send an acknowledgement message to the sender or not. If a suspicious node send a respond, it would mean that it is an authentic node but in the case of not receiving an acknowledgment from a suspicious node, it would be considered as an imminent threat and the value of the defined black hole parameter for mentioned node would be set as true.

3) Finally the identified black hole nodes are prevented access to the network and other nodes are made aware of their existence. As a result all of the packets sending toward these nodes are dropped.

We used NS2 software to simulate a ZigBee network. This simulator was operating under fedora 8 Linux OS. Then we established a black hole attack with the aid of some ID Generators. For the purpose of precision we ran the attack to the given network for twenty times then we calculated the average of those numbers. Three factors were considered in the implementation of this attack. Firstly, lifetime of the packets, secondly number of dropped packets and finally network’s throughput. These factors were examined during the intervals of 0.01, 0.02, 0.04, 0.06, 0.08 seconds. As it will be demonstrated in the comparison charts, our novel approach which is called Szigbee
HEYDARI ET AL.: INVESTIGATING THE RELATIONSHIP BETWEEN FREE CASH FLOWS AND FIRM…

(Secure ZigBee) has got optimal improvements over standard ZigBee.

**LIFETIME**

Lifetime is the existence time of a given packet in the network. Due to the fact that black hole would drop lot of packets, the lifetime of the network’s packet would diminish greatly. Packets’ lifetime are calculated with the following formula:

Equation 1. Lifetime of Packets in a network

\[
\text{ALTN} = \sum_{i=1}^{N-m} t_i + (m \times T) / N
\]

In which \(t_i\) is the death time of any \(i\) node, \(N\) is the total number of network nodes, \(m\) is the number of survived nodes after the simulation and \(T\) is the default predefined network lifetime(100s). In the following lifetime chart, there is a comparison between our novel approach which is called S-ZigBee and is one the left column of each interval with the standard ZigBee network both under the same black hole attack.

**Figure 2: Lifetime of Packets in standard and S-zigbee networks**

At the first interval, the two models have got the same lifetime, but step by step the improvement of S-ZigBee is obvious. In the last interval S-ZigBee surpass the standard ZigBee by approximately 2 seconds.

**PACKET DROP**

The second factor is the number of dropped packet in the network. In the following equation the formula for this factor is presented:

Equation 2) Packet Drop

\[
\text{Number of dropped packets} = \frac{\text{number of sent packets} - \text{number of received packets}}{\text{number of sent packets}}
\]

As we mentioned earlier the black hole node would drop any received packet so the number of a dropped packets in a network is closely dependent upon performing or preventing this attack.

**Figure 3: Number of dropped packets during transference**

In the chart above, the number of dropped packets from the start of simulation in S-ZigBee is less than standard ZigBee. In the last interval for S-ZigBee the number of dropped packets are less than half in comparison with the standard ZigBee.

**THROUGHPUT**

The number of transferred packets from sender to its destination is one of the most prominent factor in any given network. Because black hole would prevent packets from reaching their destination the throughput of a network that is entangled with black hole attack ought to be much less than an ordinary network. In the following chart the throughput of S-ZigBee from the beginning of the attack is much higher than standard ZigBee. For the first interval throughput for S-ZigBee is 1004.19(Packet per Second) while for standard ZigBee, it is 2876.56.
CONCLUSION

In this research we tried to present a novel approach against black hole attack on ZigBee networks. We simulated the attack via NS2 network simulator. Two main features of the black hole attack were considered. Firstly, the maximum of hop count for black hole nodes. Secondly, the unacknowledged nature of black hole attack. We investigated three major factors in the implementation of the attack on a ZigBee network. With the aid of demonstrated charts resulted from two attacks on standard ZigBee and S-ZigBee, from the aspects of Packet dropping, S-ZigBee had less number of dropped packet, also lifetime and throughput of S-ZigBee model surpassed the standard ZigBee.

Considering the various applications of ZigBee networks in military, industry, commerce etc. with great usage come great security threat. Although ZigBee networks are secure to most attacks, the number of attacks toward these networks are increasing rapidly. Investigating other attacks such as End Device sabotage, PiP, sniffing, spoofing and identity based attacked can be suggested for future works.

REFERENCES


implementations. Sacramento, california state
university, united states of america.

Ramesh, m. V., b.raj, a., & t., h. (2012). Wireless sensor
network security: real-time detection and
prevention of attacks. Fourth international
conference on computational intelligence and
networks pp. 785-783-787

Singhal, s., gankotiya, a. K., agarwal, s., & verma, t.
(2012). An investigation of wireless sensor
network: a distributed approach in smart
environment. Second international conference on
advance computing & communication
technologies (p. 8).

Wazid, m., katal, a., & singh sachan, r. (2013). Detection
and prevention mechanism for blackhole attack
in wireless sensor network. International
conference on communication and signal
processing,april 3-5,2013 (pp. 576-581).

zigbee security using stochastic model checking.
Lyngby,denmark: imm-technical report:issn
1601-2321