

MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey

Murat Cakiroglu
Sakarya University,
TEF Elec/Comp Dep.
Sakarya / TURKEY
muratc@sakarya.edu.tr

A. Turan OZCERIT
Sakarya University,
TEF Elec/Comp Dep.
Sakarya / TURKEY
aozcerit@sakarya.edu.tr

Huseyin EKIZ
Sakarya University,
TEF Elec/Comp Dep.
Sakarya / TURKEY
ekiz@sakarya.edu.tr

Ozdemir CETIN
Sakarya University,
TEF Elec/Comp Dep.
Sakarya / TURKEY
ocetin@sakarya.edu.tr

Abstract - *Wireless sensor networks (WSN) are very popular area of interest both in academic studies and industrial applications since they can work individually without additional maintenance and can be deployed in diverse applications. However, the limited source of the nodes cannot guarantee a sufficient level of security and also complicates the design and the implementation of the algorithms/protocols. In the WSN, Medium Access Control (MAC) protocols have a special significance that it helps maintaining the communication resources effectively. In this paper, we have summarized the Denial of Service (DoS) attacks threatening MAC protocols followed by an investigation on protocols designed against to DoS attacks and finally open research issues have been studied on secure MAC designs.*

Keywords: DoS, MAC, Wireless Sensor Networks.

1 Introduction

WSNs consist of sensor nodes with limited capacity, low power and low cost, and communicating relatively in short distance over wireless medium [1]. The nodes are scattered randomly into target field where they can identify each other, monitor and report the surrounding properties by means of they are assigned. WSNs can be used many diverse areas from hospitals and emergencies to military and defense applications.

Since sensor nodes have limited and irreplaceable power supplies, the most crucial restriction for nodes is low power dissipation requirements. Because mostly power supplies determine the total life cycle of the node and the network as well, WSNs should dissipate low power and deployed protocols/algorithms should be power sensitive [3]. The most power dissipating processes are data transmitting, data receiving, and idle listening. Therefore, MAC protocol is one of the key concerns determining nodes' life cycle in the wireless network. Another complicated design issue is to maintain the security functions for the period of the life cycle of the network. Limited hardware/software resources and hostile environment can make the nodes vulnerable to physical damage and compromising. In this paper, we have investigated MAC protocol security problems and analyzed

proposed solutions. The rest of the paper is organized as follows. In Section 2, we summarize the details of basic wireless MAC protocols. Section 3 explains the type of DoS attacks on MAC layer. We analyze proposed and designed DoS resistant protocols in Section 4. In Section 5, we conclude the paper with open research issues on secure MAC protocols in the WSN.

2 MAC Background

MAC protocol is an aggregation of rules maintaining fair and efficient use of the shared channel. Several MAC protocols used in the wireless networks have been proposed [9] however, since proposed protocols are designed for traditional wireless networks, it is not reasonable to use them without appropriate modification in the WSNs. Because the WSNs have a wide range of applications and there is no approved standard on sensor nodes' hardware have prevented from developing a standard MAC protocol for WSNs. In this section, S-MAC, the most common MAC protocol designed for WSNs, is explained.

S-MAC (Sensor MAC)

S-MAC is based on the 802.11 protocol, but it differs from the 802.11 protocol in a way that instead of listening to the medium constantly, it does listen to the medium periodically with listen/sleep modes in order to lower energy consumption [2]. Because of energy limitation of the nodes, in S-MAC protocol the power dissipation is preferred as the most significant criterion. In addition to periodic listen/sleep mechanisms, collision/overhearing avoidance and message passing methods are applied to sustain minimum power dissipation.

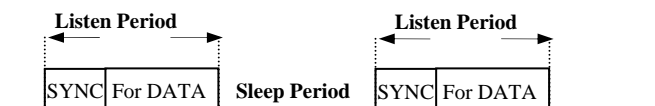


Figure-1. S-MAC

In S-MAC protocol, the nodes listen to the medium in time slots and, they only communicate with their neighbors as required. In idle state, they switch to the sleep mode in which the energy saving can be possible since the

transmitter/receiver units are off. Periodic listen/sleep modes, however, require periodic synchronization to eliminate negative effect of clock drifts. In S-MAC protocol, neighbor nodes creating virtual cluster use same listen/sleep timing. Synchronization is maintained between listen/sleep time slots using small control packets called as SYNC. In addition to physical and virtual carrier sense, RTS/CTS (Request To Send/Clear To Send) control packets are used to avoid collision. By enabling interfering nodes to switch to sleep mode after they hear an RTS/CTS packet, the overhearing problem is overcome. Another significant property of the S-MAC protocol is message passing method in which large data packets are fragmented into small packets and sent out in burst with only one RTS/CTS control packet.

3 MAC Layer DoS Attacks

The remote sensor nodes deployed in an environment may object to physical damage and may be reprogrammed for undesirable purposes by hostile people who can locate attacker nodes randomly into the nodes to disturb the communication between nodes by radio interferences. These sorts of attacks are called as jamming style DoS attacks and the purpose of them is to disrupt the communication and mission of clusters or the whole network. In WSNs, DoS attacks are intended for physical, data link, routing and transport layers [7]. In this paper, we have investigated the DoS attacks of disrupting medium access decreasing band utilization and increasing power dissipation.

3.1 Classification of DoS Attacks and Jammer Models

DoS attacks are divided into three groups on MAC layer [7] and four individual types of jammer model are derived [10].

Collision Attacks and Reactive Jammer

Jammer node/nodes check the communication channel to ensure whether the medium is busy. If so, jammer assumes that the RTS/CTS or data packets are in the medium, therefore, it sends out jamming packets to collide with legal packets. Corruption on an octet of the packet requires retransmitting of the entire packet. As shown in the Figure-3, reactive jammer uses this type of attack. Reactive jammers listen to the channel constantly and therefore, they are not power efficient but they are hard to detect since they don't attack all the time.

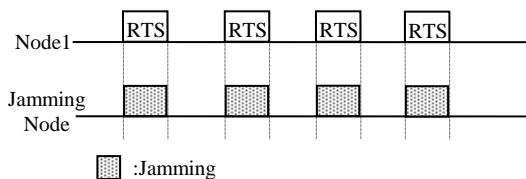


Figure-2. Transmission failure caused by reactive jammer

Unfairness Attacks and Constant, Random Jammer

Each node has equivalent priority over the use of the medium in the RTS/CTS based medium access protocols. Since the first node gaining access to the medium has right to send out packets, a fair channel sharing is possible. Utilizing this attribute the attacker checks the medium availability and send out packets without delay or repeatedly. In doing so, the channel is utilized by the attacker/attackers instead of legal nodes. Constant and random jammers use this type of attack. Constant jammer without having a MAC label generates random number of bits and make busy of the medium. The random jammer on the other hand, attacks in specified intervals then switches to the sleep mode, therefore, the power dissipation is relatively less than others. The duration of attack and sleep can be varied randomly.

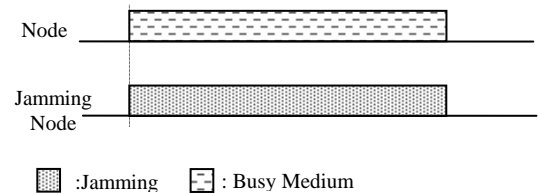


Figure-3. Constant Jammer

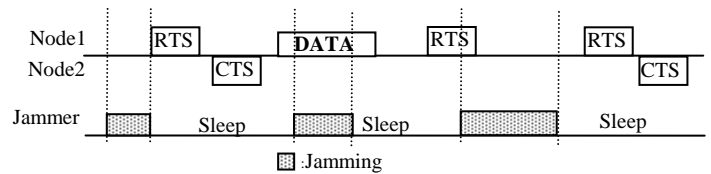


Figure-4. Random Jammer

Exhaustion Attacks and Deceptive Jammer

In RTS/CTS based medium access protocols, the sender releases an RTS packet to transmit a data packet and the receiver releases a CTS packet in response. By sending out many RTS packets, the attacker node forces the receiver to send out CTS packets, consequently the attacker causes the receiver to exhaust its entire power. Deceptive jammer uses this type of attacks and tries the receivers to be in receiving mode by sending out legal packets constantly.

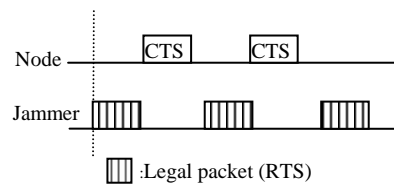


Figure-5. Node in receive mode due to deceptive jammer

4 DoS Resistant Protocols for WSN

There are not many studies related to DoS resistant protocols for WSNs. In this section, we summarize a variety of protocols developed against to MAC layer DoS attacks.

4.1 JAM (Jammed-Area Mapping)

A mapping protocol is designed against to MAC layer DoS attacks. The nodes decide to whether they are under attack by the help of a software based jamming detection module inside in each node [4]. The parameters used to detect the attack are: repeated inability to access wireless channel, bad framing, checksum failures, illegal values for addresses or other fields, protocol violations, missing ACKs), excessive received signal level, low signal-to-noise ratio, repeated collisions, and duration of condition.

As shown in Figure-7, by releasing JAMMED messages, the jammed nodes announce to neighbor nodes that they are under attack. Under attack condition, it is very hard to send out a message for a node since the medium is occupied by the attacker. In order to overcome this obstacle, the JAMMED message should be prioritized, that is, the MAC protocol must be modified accordingly. Neighbor nodes received JAMMED messages exchange BUILD messages and list the jammed nodes, thus, the jammed region is determined. Having recovered from the attack, the jammed node sends out an UNJAMMED message in response and TEARDOWN messages are exchanged by neighbor nodes receiving UNJAMMED messages to update the jammed node list. As a result, an adaptive quarantine region can be established. The data flow in the sensor network may not be blocked by use of feedback which is generated from mapping protocol. Furthermore, it can be prevented from the attack by transferring related feedback information on attack to the central management stations i.e. base stations. The region can be quarantine in 1 to 5 seconds and the protocol can continue to operate securely up to 25% failure rate. However, there has been no real system deployed with JAM protocol yet, the implementation phase is accomplished by software based simulation tools.

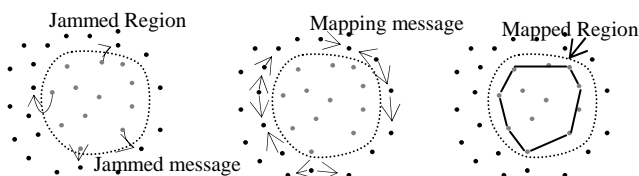


Figure-6. Mapping a jammed region in the network [4]

4.2 FSMAC

FSMAC [5] is made up with intrusion detection and defense modules in addition to the 802.11 MAC protocol.

Each node having these modules, determines the presence of attacks statistically. More number of collisions implies collision attacks, more RTS packets implies exhaustion attacks, more average waiting time for packets on the MAC layer implies unfairness or collision attacks. The fuzzy logic method is used to determine the attack's existence. If any type of the attack of the three is present, the paper suggests that jammed nodes switches to sleep mode and checks the attack's presence by awaking with specified intervals. Another solution to the problem is to change the RF band of the node, at present however, this is not viable function for sensor nodes, which operates on a single channel frequency.

4.3 G-MAC

The G-MAC [6] uses central group method against the DoS attacks. Nodes in group, uses the gateway sensor (GS) only to communicate with other nodes in the group. The packets received from other sources are disregarded, thus, deceptive jammer attacks are avoided. However, this protocol cannot maintain security against constant jammers, random jammers and reactive jammers. In G-MAC, a frame is divided into two periods, namely collection and distribution. In collection period the group manager, which is called as gateway node, collects and manages the intra-network and inter-network traffics and switches to the sleep mode afterward. GS initiates the distribution period by releasing GTIM (Gateway's Traffic Indication Message) message, which declares successive collection and distribution periods. GS node is chosen periodically according to the energy levels of nodes.

4.4 Further Studies for DoS Attacks on MAC Layer

As cited in the Section-3, Wenyuan Xu, et al. [10] describes four types of attackers and develops some methods to determine them. The first method depends on obtaining the signal strength statistically. It is reasonable to consider that abnormal values in the signal power distribution indicate a high risk of an ongoing attack. Nevertheless, W. Xu reports that there are difficulties to differentiate between attacks scenarios and legal traffics in definite terms by means of merely signal power level measurements in the experiments. The second method is to measure the carrier sense intervals. In the presence of an attack the carrier sense interval is extended, but the interval can also be extended by a bottleneck. To differentiate between the two intervals, a calculated threshold value from the network models can be used. However, these methods also cannot allow determining random jammer attacks and reactive jammer attacks. Another method is to check the Packet Delivery Ratio (PDR), which differentiates between a bottleneck and an attack, cannot also determine the use of bad connections whether it is originated from attacks or nodes' movement. Because of

inability to determine the type of attacks by three proposed methods, W. Xu et al. have suggested two new attack determining protocol using consistency check. In the first protocol, the determination is made by the relation consistency between signal power measurement and packet delivery rates as shown in the Table-1.

Table-1: The relation consistency determination

| Packet delivery rate | Signal power | Interpretation |
|----------------------|--------------|--|
| 0 | LOW | Originated from neighbor node fault i.e. end of life cycle |
| 0 | HIGH | Node under attack |
| LOW | LOW | Neighbor nodes are far from transmitting area |
| LOW | HIGH | Node under attack |

In the second protocol though, the location data and PDRs of the nodes are used. Nodes announce their location to their neighbors periodically and every node stores their neighbor location data and PDR values. In this way, it is expected for neighbor nodes having close values, and any inconsistency among them indicates an attack condition. In another paper [8], energy effective attack types are developed for S-MAC, L-MAC, B-MAC by investigating of the packet arrival intervals, and the type of attacks cited in Section-3 are utilized in this study.

5 CONCLUSION AND OPEN RESEARCH ISSUES

There are not many studies related to medium access protocol producing a robust solution against to the MAC layer DoS attacks. WSNs must be robust and secure enough against to attacks especially as in military applications, building security systems, biologic and chemical hazard warning applications. Wireless sensor nodes that have insufficient hardware sources are quite vulnerable against to DoS attacks especially if the energy consumption is preferred as the most significant design criterion. Since sensor nodes use almost a single channel frequency to communicate and have insufficient hardware to implement complex functions like CDMA, the designers are directed towards the solutions present today. As explained in Section-4, FSMAC suggests frequency hopping or sleeping of nodes solutions after determining an attack. Meanwhile, the frequency hopping technique is not used for commercial nodes and for most scenarios switching nodes to sleep mode causes impediment of the network functions and dependability problems. G-MAC can prevent from only one type of attack using central gateway function, so full security cannot be established by G-MAC. JAM protocol determines and quarantines the attacked regions. It assumes that the attackers are placed on only a part of the network and the communication continues in the unaffected regions. This approach rather generates defensive mechanisms. Also, in [10] and [8],

DoS attack models on MAC layer and determination of attackers are investigated. Although TDMA (Time Division Multiple Access) based DoS attacks have been developed [12], TDMA based TRAMA and BMA protocols are more robust to DoS attacks compared to CSMA (S-MAC, T-MAC) based protocols. The nodes should be redesigned against to DoS attacks especially on physical and MAC layer. Additional integrated hardware and software units with low power and low cost are required to determine the attack and to defense the network.

6 REFERENCES

- [1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, Vol. 38, No. 4, pp. 393-422, March 2002.
- [2] Wei Ye, J. Heidemann, Deborah Estrin. An energy-efficient mac protocol for wireless sensor networks. IEEE Infocom, pages 1567-1576, NY, June 2002.
- [3] I. Demirkol, C. Ersoy, and F. Alagöz, "MAC Protocols for Wireless Sensor Networks: a Survey," IEEE Communications Magazine, (IN PRESS), 2005
- [4] A. Wood, J. Stankovic, and S. Son. JAM: A jammed-area mapping service for sensor networks. In 24th IEEE Real-Time Systems Symposium, pages 286-297, 2003.
- [5] Q. Ren, Q. Liang, "Fuzzy logic-optimized secure media access control (FSMAC) protocol", CIHSPS 2005, 31 March-1 April 2005 Page(s):37 - 43
- [6] Brownfield M., Y. Gupta, Davis N, "Wireless sensor network denial of sleep attack", Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. 15-17 June 2005 Page(s):356 - 364
- [7] A.D.Wood and J.A.Stankovic, "Denial of service in sensor Networks", IEEE Computer, 35(10):54-62, Oct. 2002.
- [8] Yee Wei, L. Lodewijk, V. Hoesel, J. Doumen, P. Hartel, P. Havinga, "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols SANS'05, November 7, 2005, Virginia, USA.
- [9] Sunil Kumar, Vineet S. Raghavan, Jing Deng "Medium Access Control protocols for ad hoc wireless networks: a survey" Ad Hoc Networks, ELSEVIER
- [10] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc '05, page To appear. ACM Press, 2005.