Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 69 (2014) 22956-22960

ISSN: 2229-712X

Analysis of security mechanisms against Denial-of-Service attack in wireless sensor networks

C K Marigowda and Sunanda Golgeri

Department of Information Science & Engineering, Acharya Institute of Technology, Bangalore, India.

ARTICLE INFO

Article history:

Received: 13 February 2014;

Received in revised form:

20 March 2014;

Accepted: 3 April 2014;

Keywords

Wireless Sensor Networks,

Denial of service,

Reply,

Jamming attack.

ABSTRACT

Wireless Sensor Networks are used in numerous security sensitive applications, it composed of a huge number of resource limited sensors therefore we should make sure the network is secured against security attacks. Denial of service attack in WSNs is a serious attack that reduces the network capacity dramatically and the users fail to receive expected service. Many schemes have been proposed to tolerate or destroy DoS attack, but very few can identify intruders and provide security against this attack. In this paper, we explore the effects of DoS in WSN, effective security methods for achieving the security against this attack. Finally two important types of DoS attacks called jamming and reply attack are studied and possible solutions are recommended.

Introduction

In Wireless sensor networks, sensor nodes monitor the physical conditions, detect different types of events of interest, produce data, and collaborate and forward it toward a sink, which could be a gateway or base station. Figure.1 shows the general architecture of WSN [8]. The data is forwarded through multiple hops to a sink may use it locally, or through gateway it may connected to other networks.

Sensor nodes have self-organization capability, low cost and easy to deploy therefore sensor network is often deployed in an unattended environment to perform the data collection and monitoring tasks. An attacker may launch various attacks to disrupt the network communication by compromising nodes when sensor nodes are distributed randomly in unguarded environment. Among these attacks, common ones are DoS, reply and jamming attack. The DoS attack destroys or diminishes network capacity of the network by interferes with the radio frequencies that network's nodes are using. Jamming attack eliminates a network's capacity to perform its expected function and reply attack floods network with bogus packets so the packets are continuously replayed back to the sink node.

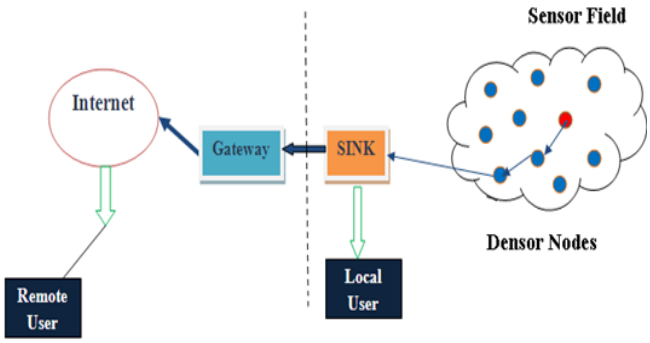

Figure.1: WSN Architecture

The rest of this paper is organized as follows. In Section 2, Denial of service attack, DoS attack on different layers and important security schemes are discussed. The major DoS attack is jamming attack which present at the physical layer, different types of jamming attack and security mechanism against this attack discussed in Section 3. In Section 4, one more important DoS attack such as reply attack and some security methods against reply attack are discussed. We conclude the paper in Section 5.

Denial of Service Attacks in WSNs

The DoS attack defines an adversary's attempt to destroy a network; DoS attack can be defined as any event that diminishes network's capacity by compromising nodes to perform requested function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS attack.

Layer wise DoS attacks in WSN: Issues and Mitigation mechanisms

Layer wise categorization of DoS attacks was presented by Wood and Stankovic [1]. Raymond and Midkiff [2]. In this section, we discuss current DoS attacks based on various protocol layers and their security mechanisms in wireless sensor networks [4].

DoS attacks on the physical layer

Jamming and node tampering attacks are two well-known DoS attacks in the physical layer [5]. Jamming means the intentional interference with radio reception to oppose a target's use of a communication channel. Different types of jamming such as Constant, Deceptive, Random, and Reactive [3] attacks are present and are difficult to handle in case of sensor networks. In node tampering attack an attacker can derive sensitive information such as security keys or other important information of node [6].

DoS attacks on the link layer

The attacks when situated on this layer results in collision, exhaustion, unfairness, interrogation. Collision occurs when two nodes simultaneously attempts to transmit on the same frequency, Resource exhaustion of network resources by inducing repeated retransmission attempts and unfairness in allocation of frames, Unfairness which is considered a weak form of a DoS attack can be performed by attacker attempt to

Tele:

E-mail addresses: marigowda@acharya.ac.in

degrade the network performance instead of completely preventing access to a service [6].

DoS attacks on the network layer

Network layer is exposed to different types of attacks such as alter routing information, selective forwarding, sinkhole, Sybil, wormhole, hello flood and acknowledgment flooding attack [5]. In order to increase traffic in the network, attacker may alter routing information. These disruptions include the creation of routing loops, extending and shortening source routes, attracting network traffic from select nodes, generating false error messages, increasing end-to-end latency and extending and shortening source routes and partitioning the sensor network [6].

DoS attacks on the transport layer

There are two critical attacks in transport layer they are flooding and de-synchronization attack [6]. In flooding attack an adversary make connection requests frequently until the resources required for each connection reach a maximum limit. De-synchronization attack disturbs an existing connection. An attacker may repeatedly send messages to an end host making that host to request for the missed frames retransmission [8].

DoS attacks on the application layer

Overwhelm attack is the one main attack in application layer. Here an attacker flood the nodes with sensor stimuli it causes the sensor network to forward large volumes of traffic to base station. This attack consumes more node energy and network bandwidth [6,7,8]. In application layer buffer overflow occurs and it is vulnerable to logic errors. The Table.1 lists the DoS attack on different layers of WSN.

Layers	Attacks
Physical Layer	Jamming
MAC/Data Link Layer	Collision
	Reply
	Exhaustion
	Unfairness
Network Layer	Spoofed routing information and selective forwarding
	Sink hole
	Sybnil
	Wormhole
	Hello flood
	Ack. flood
Transport Layer	flooding
	De-synchronization

Table 1: Denial of Service Attacks on Sensor Network Layer

Defense Strategies against DoS attack in WSNs

There is very little work done on the prevention of DoS attacks. Existing protocols often focus on cryptographic-authentication mechanisms to provide DoS resilience. Currently there are four mechanisms that could be helpful to overcome DoS attacks in WSN:

Watchdog scheme: To overcome from DoS attacks in WSNs the necessary operation is to identify and mitigate the misbehaving nodes. Watchdog scheme can achieve this purpose through using watchdog and pathrater concepts. Every node implements a watchdog that constantly monitors the packet forwarding activities of its neighbors and a path-rater rates the transmission reliability of all alternative routes to a particular target node. The disadvantages of this method are that (1) fails to detect misbehavior or raise false alarms in the presence of ambiguous collision, receiver collision and limited transmission power (2) and it is applicable only for source routing protocols not for general routing protocol [6].

Rating scheme: In rating scheme neighbors of a node collaborate to rate the node according to how well the node performs the functions requested from it such as packet forwarding and not at disrupting the flow of information in the network by intension [18]. The disadvantages of this method are (1) how the evaluated node function result can be evaluated by an evaluating node, (2) evaluated node may be able to cheat easily, and (3) the function result requires remarkable overhead that has to be exchanged to the evaluating node [6].

Virtual currency: Virtual currency systems use credit or micro payments to compensate for the service of a node. A node receives a virtual payment for forwarding the message of another node, and this payment is deducted from the sender or the destination node. Two examples of such systems are: Nuglets and Sprite. Nuglets has two models: Packet Purse Model and Packet Trade Model. The advantage of Packet Purse Model is that it prevents jamming the network from users and the source node may not know how many Nuglets need to be loaded into the message. In sprite, the sender is charged to prevent a denial-of-service attack to the destination by sending it a lot of traffic. The disadvantages of this scheme are: (1) harmful jamming of the network cannot be prevented (2) intermediate nodes can take out more number of Nuglets than they are assumed and (3) overhead [16].

Route DoS Prevention: This method attempts to prevent DoS in the routing layer by cooperation of multiple nodes [17]. The drawback is legitimate nodes can be classified as misbehaving nodes but happens very rarely. Here a pair of nodes establishes a certain application specific level of protection before any security-sensitive traffic begins.

Here we discussed four important mechanisms to overcome DoS attack among these Route DoS prevention scheme is best suitable to provide security against DoS attack because that incorporates a mechanism to assure routing security, fairness and robustness targeted to mobile ad hoc networks this feature is not present in rest of the three schemes.

Reply attack in WSN

In DoS attack one form attempts to disrupt the network service, may be by blocking communication between nodes [8]. The other form of DoS attack is the path-based DoS (PDoS) attack where the network is flooded with bogus packets along a multi-hop data delivery path. The packets are continuously replayed back to the sink node. This attack is known as reply attack. The objective of such attacks is to eliminate or diminish the network performance and thereby hamper the working of the whole system [9]. Figure.2 shows compromising beacon nodes or replying beacon packets that user intercepted in different location. So, non beacon nods will determine their location incorrectly.

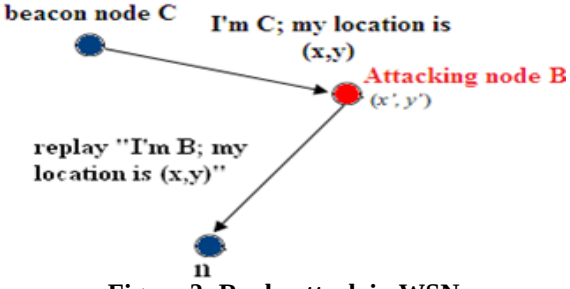

Figure.2: Reply attack in WSN

Defense strategies against Reply attack in WSNs

Authentication protocol is proposed by the authors in [10] capable of resistance against reply attacks and other DoS attacks. But the scheme uses symmetric keys where keys are shared by sensor nodes and compromised node can send fake messages which may have a great security threat to the network.

The authors in [11] have devised a mechanism to prevent reply attacks. They considered that the packets used for time-synchronization of any two nodes are replayed. The receiving nodes will adjust their clocks depending on the arrival time of the beacon message by using receiver-receiver model. A time offset is calculated based on the difference between the recording times of the beacon message by these receiving nodes. The time offsets are exchanged between the receiving nodes to calculate a threshold value which is the difference between the two time offsets of two nodes. But the arrival of a beacon message at a node can be delayed by certain factors leading to gross errors while deriving the time required for synchronization between the nodes. Moreover, by not using global time synchronization model a large overhead has been introduced as huge number of time offsets need to be computed by the nodes.

Dong et al. have proposed the use of hash chains in their work where each node combines the hash value with its own node-id and forwards this combined value to its next higher hop count node. The receiving node is able to detect reply attacks by observing the combined value of node-id and hash value. But the computation of all these values by nodes takes significant amount of time [12].

To defend against reply attacks Soroush et al. [13] have developed a scheme where increasing counter is maintained to keep track of old replayed messages. And each node maintains a counter to store the timing information of all other nodes which requires a large amount of memory leading to a major bottleneck for memory-constrained sensor nodes.

Zero Knowledge Protocol (ZKP) is one method to defend against reply attack. In reply attack, an intruder tries to reply the prior communication and authenticate itself to the verifier. But, in this model verifier will send different values each time in communication, and replays for earlier communication. Key exchange, Detection and other basic cryptographic operations is allowed mainly by Zero Knowledge Protocol. However, there is no unanimity on whether reply protection should be implemented at the link layer or at the application layer in WSN [7]. SPIN protocol also provides security for Reply attack in WSNs. SNEP is part of SPINS and is one of the first attempts to implement a secure link layer protocol. It achieves reply protection by keeping a consistent counter between the transmitter and receiver [15]. MiniSec is a secure link layer protocol provides two different strategies for reply attack for its two different operating modes [14] such as MINISEC-U and MINISEC-B. The receiver keeps two alternating Bloom filters, one for the current interval and one for the previous period. When it receives a packet it queries the corresponding Bloom filter whether the packet already exist or not and if the query returns true, then that packet is considered to be a reply. The problem, however, is that the Bloom filters may cause a legitimate packet to be rejected as a replayed packet .

ZigBee protects against message reply attacks. In wireless sensor network ZigBee security protocol is used to provide confidentiality and integrity, as well as defense against reply attack. Furthermore, AES algorithm provides confidentiality, CCM mode is apply for integrity, and frame nonce is checked to prevent reply attack. However, ZigBee is a costly protocol [8].

In this section we discussed different security mechanisms to defend against reply attack in WSN by comparing all these methods we conclude that Zero Knowledge Protocol (ZKP) has high cryptographic strength. As the value of public key get changed with every communication so it becomes extremely difficult for the attacker to break the security. The model uses finger print for each and every communication between the nodes. Thus it is easy for the administrator to identify these attacks using ZKP.

Jamming attack in WSN

In WSNs Jamming is a type of attack which interferes with the radio frequencies that network's nodes are using. Because physical layer is lowest among all WSNs layer therefore it is the first layer attacked from jammers. Figure.3 pictorially describes the jamming attack on sensor network. The malicious node X jams the normal nodes C and D has been jammed by, so the communications between the jammed nodes(C, D) and the normal nodes (A, B, E, H, I) are disrupted. Different types of jamming (Constant, Deceptive, Random, and Reactive) are present and are difficult to handle in sensor networks they are discussed here [6].

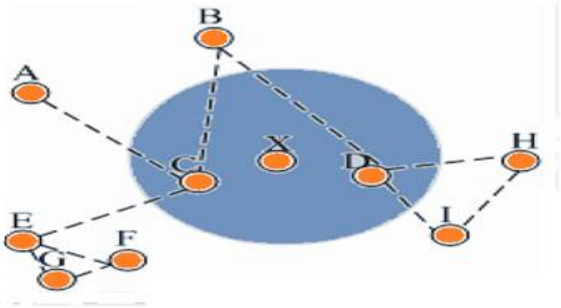

Figure.3: Jamming Attack in WSN

Constant jamming: This attack is one of the most effective jamming attacks it reduces the network throughput down to zero until the jammer stops jamming either runs out of energy or attack is detected. This attack is very strong it makes the transmitter to sense the medium as busy most of time and will therefore drops the messages.

Deceptive jamming: Deceptive jammer is the one that transmit semi-valid packets. Semi-valid packets means here is packet header is valid but the payload is of no use. To carry out this attack and track communication deceptive jammer only need to know hop sequence which is based on pseudo random number. And pseudo random sequence is easy to solve therefore with less cost this attack can be introduced.

Random jamming: Random jammer is constant jammer or deceptive jammer because it has characteristics of both constant jammer and deceptive jammer. Random jammers are more energy efficient compared to other jammer but a little less efficient to reject service. This jamming consists of two alternate modes. In the first mode jammer jams for arbitrary period of time it can behave either constant or deceptive jammer, and in the second mode the jammer go to sleep mode it turns off its sender for another arbitrary period of time. This attack saves energy and makes difficult to detect.

Reactive jamming: In Reactive jamming target is receiver. A reactive jammer jams the network when it knows that a device is transmitting in order to minimize energy required for it. This attack modify sender bits by introducing more noise in order to alter bits only a minimum amount of power is required to alter bits. When modified bits arrive at receiver it will consider packets as invalid and discard the packets.

Defense Strategies against Jamming attack in WSNs

A jamming source either powerful enough to disrupt the entire network or less powerful to interrupt a smaller port of the network. Even with lower powered jamming sources, such as a small compromised subset of the sensor nodes, an attacker has the potential to disturb the entire network provided the jamming sources are randomly distributed in the network. Therefore jamming attack in WSN is more powerful and a comprehensive mechanism required for mitigating this attack. There are solutions available to defend against jamming attacks in WSN. The most popular protection against jamming attack is spread-spectrum communication scheme

Frequency-Hopping Spread Spectrum (FHSS)

It is a spread-spectrum method by using a shared algorithm known both to the sender and the receiver transmitting radio signals by rapidly shift carrier among many frequency channels. FHSS brings forward many advantages in WSN environments:1)It minimizes unauthorized interference and jamming of radio transmission between the nodes.2)The SNR required for the carrier, relative to the back-ground, decreases as a wider range of frequencies is used for transmission.3)It deals effectively with the multipath effect.

One of the main drawbacks of frequency-hopping is that the overall bandwidth required is much larger than required Multipath in wireless telecommunications. In general, to maintain low cost and low power requirements, sensor devices are limited to single-frequency use and are therefore highly vulnerable to jamming attacks [6, 7, 8].

Direct Sequence Spread Spectrum

In Direct Sequence Spread Spectrum (DSSS) transmissions are performed by multiplying the data that is to be transmitted and a Pseudo-Noise (PN) digital signal. The PN digital signal means pseudo random sequence of values at a frequency higher than original signal. DSSS also provide above mentioned advantages of FHSS. DSSS makes the attacker to decode signal difficult. Also since the transmitted signal of DSSS resembles with noise, radio direction finding of the transmitting source is a difficult task. [6,7,8].

Directional Transmission

The use of directional antennas could dramatically improve jamming tolerance in WSNs. In general directional antennas/transmission provides better protection against eavesdropping, detection and jamming than omni-directional transmission. A directional antenna transmits or receives radio waves only from one particular this feature allows increased transmission performance, more receiving susceptibility and reduced interference from unwanted sources compared to omnidirectional antennas. The main drawback of directional transmission is the requirements of advanced MAC protocol and multipath routing.

Ultra Wide Band Technology

Ultra Wide Band (UWB) technology is a modulation technique based on transmitting very short pulses on a large spectrum of a frequency band simultaneously. This renders the transmitted signal very hard to be intercepted/jammed and also resistant to multipath effects. In the context of WSNs, UWB can provide many advantages such as it promises low power and low cost wide deployment of sensor networks. In addition, UWB based sensor networks guarantee more accurate localization and prolonged battery lifetime.

Different security mechanisms against jamming attack is explained in this section compared to all above mechanism FHSS brings forward many advantages in WSN environments:

• It minimizes unauthorized interception and jamming of radio transmission between the nodes.
• The SNR required for the carrier, relative to the background, decreases as a wider range of frequencies is used for transmission.
• It deals effectively with the multipath effect.
• Multiple WSNs can coexist in the same area without causing interference problems.

The first three of the above-mentioned FHSS advantages also apply to DSSS. Furthermore, the processing applied to the original signal by DSSS makes it difficult to the attacker to descramble the transmitted RF carrier and recover the original signal. Also since the transmitted signal of DSSS resembles white noise, radio direction finding of the transmitting source is a difficult task. On the contrary due to the limited supported chip rate (2 Mchip/s) and the restricted transmission power of sensor nodes (typically 0 dBm) the network is very likely to collapse under a jamming attack.

Conclusion

The deployment of sensor nodes in an unattended environment makes the networks vulnerable, therefore security is of main concern while using wireless sensor networks. This paper conducts a survey of the wireless sensor networks security threat such as Denial of service, reply attack and jamming attack, and to provide security against such attacks by proposing some of the important security mechanisms. As DoS attack covers a large number of attacks and threats in WSN, finding efficient mechanisms for effective prevention of DoS situations still remains an open research issue. This survey will help the researchers to come up with efficient and more robust security mechanisms and make their network safer.

Reference

[1] Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher," Wireless Sensor Network Architecture", International Conference on Computer Networks and Communication Systems, 2012.

[2] M.D.Pardue, "Fine-tuning the OSI model: Layer functions and services," in Military Communications Conference - Crisis Communications: The Promise and Reality, 1987, IEEE, vol. 1, Oct. 1987 pp. 0199-0203.

[3] Haider Qleibo," Message integrity model for wireless sensor networks",2009 Salvatore La Malfa, "Wireless Sensor Networks",2010.

[4] Anthony D. Wood and John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks".

[5] Huda Bader Hubboub, "Denial of Service Attack in Wireless Sensor Networks",2010

[6] Abdulaziz Rashid Alazemi, "Defending WSNs against jamming attacks", Journal of Networks and Communications 2013; 2(2) : 28-39American

[7] Manish P, Gangawane," Implementation Of Zero Knowledge Protocol In Wireless Sensor Network for Identification Of Various Attacks", International Journal of Emerging Technology and Advanced Engineering, August 2012 Volume 2, Issue 8.

[8] Devesh C. Jinwala, Dhiren R. Patel,"Optimizing the Reply Protection at the Link Layer Security Framework in Wireless Sensor Networks".

[9] M .Yasir Malik, "An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations".

[10] Liu D, Nin P "Efficient distribution of key chain commitments for broadcast authentication in distributed WSNs". In: tenth annual Network and Distributed System Security Symposium, 2003, pp. 263–276.

[11] Song.H, Zhu.S, Cao.G: "Attack resilient time synchronization for WSNs". In: IEEE International Conference on Mobile- Adhoc and Sensor Systems Conference, 2005, vol. (7-7), pp. 772–779.
[12] Dong. J, Ackermann.K.E, Bavar, B., Nita-Rotaru, C.: Mitigating Attacks against Virtual Coordinate Based Routing in Wireless Sensor Networks. In: Proceedings of 1st ACM conference on Wireless Network Security, 2008, pp. 89–99
[13] Soroush, H, Salajegheh, M, Dimitriou T: Providing Transparent Security Services to Sensor Networks. In: IEEE International Conference on Communications, 2007, pp. 3431–3436.
[14] Poisel Richard, "Modern communications jamming principles and techniques".
[15] Dr. Banta Singh Jangra, Vijeta Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology, September 2012 , (IJEIT) Volume 2, Issue 3.
[16] F.Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks", Ad Hoc Networks, vol. 3, issues 1, 2005, pp. 69-89.
[17] A. Agah and S. K. Das, "Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach", International Journal of Network Security, Sept. 2007, vol.5, no.2, pp.145–153.
[18] Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma, "Secure Wireless Sensor Networks: Problems and Solutions", systemics, cybernetics and informatics volume 1 - number 4