March - April 2020
ISSN: 0193-4120 Page No. 10671 - 10677

A Review on detection mechanisms used in Wireless Sensor Network for DoS attacks

Dr. KanagaSuba Raja S[1], Sobini X. Pushpa[2]
[1]Easwari Engineering College, Chennai.
[2]St.Xavier's Catholic College of Engineering, Nagercoil.

Article Info
Volume 83
Page Number: 10671 - 10677
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 13 April 2020*

Abstract: Wireless sensor networks are growing because of their effectiveness and low cost. WSN consists of numbers of small sensor nodes which are deployed in remote areas to sense real-time events. Collected information are processed and transmitted to base stations for further processing. Nowadays wireless sensor network became the key technology for Internet of Things. Sensor nodes are with limited resources and power. Providing security mechanisms as in wired network will not work for WSN because of limited resources. So protecting sensor network from various attacks is a difficult task. Denial of Service (DoS) attack is one which denies a network to provide its intimate service to the end user. DoS attacks takes place in different layers of sensor network architecture. For the detection of DoS attack lot of authentication algorithms are proposed so far. This paper presents a detailed review on various detection mechanisms used nowadays to detect DoS attacks in the WSNs.

Keywords:*Wireless sensor network, Denial of Service attack.*

I. Introduction

Wireless sensor network is nothing but a network with thousands of sensing devices which are deployed in remote areas to sense the environmental changes and to transmit the sensed data to base stations in which they are connected to. Here the nodes are deployed in random manner, so care should be taken while deploying the nodes. If distance between nodes is more network coverage problem will occur, if distance is low network will not be efficient due to heavy traffic. Data collected by sensor devices are highly sensitive and can be easily affected by intruders. So WSN should have more effective security mechanisms when compared to wired network.

Wireless sensor network architecture follows OSI layer model. In general WSNs protocol stack has 5 major layers and 3 cross layers. Major reason behind this layered approach is to increase the complete efficiency of the network and to protect the sensor node from different types of attacks. Each layer is responsible for different tasks independently of the other layers in the protocol stack such as Transport layer is responsible for reliable data transfer, Network layer is responsible for routing, Data link layer is responsible for data multiplexing and error control, Physical layer supports data transmission over physical medium and application layer is used for traffic management. Like that 3 cross layers are responsible for power management mobility management and task management.

March - April 2020
ISSN: 0193-4120 Page No. 10671 - 10677

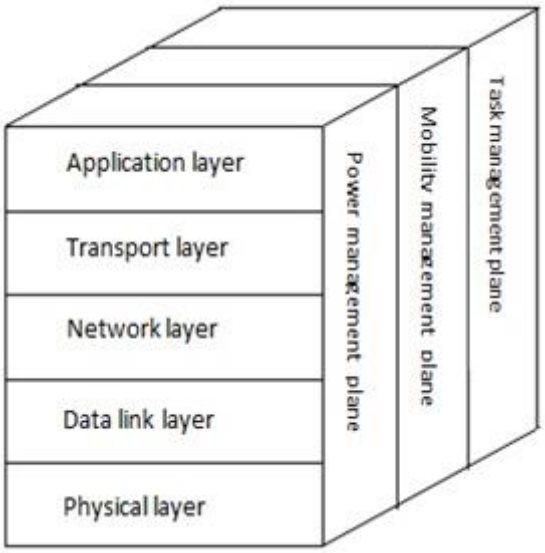

Fig: 1 Protocol stack of WSN

Issues in providing security to WSN

Nodes in sensor network are resource constrained. They have low processing capability, limited battery power, low storage capacity, limited energy and limited communication bandwidth [1]. Communication from one sensor node to another sensor node is costlier than instructions computation [5]. General obstacles in providing security to sensor nodes are listed below:

1. Limited resources:

a) Memory: Usually flash memory and RAM will be used in sensor nodes. Downloaded application codes are stored in flash and RAM is used to store sensor data and for intermediate computations. Enough memory space will not be there to run complex algorithms and complicated computations after installing OS. So it is difficult to use standard security algorithms in WSN [1].

b) Processor: Processors in sensor nodes are not that much powerful as in wired or ad-hoc network nodes. It should also consume less power. So complex cryptographic algorithms cannot be used in WSN [1][3].

c) Battery: Sensor networks are powered by batteries. Life of a sensor network depends on the battery power of the nodes in the network. Data communication between nodes and data processing consumes more power. So care should be taken while selecting security mechanisms. That is asymmetric cryptography algorithms are more expensive so efficient symmetric cryptographic algorithms can be used in WSNs to consume less power [4] [2].

2. Dynamic topology: WSN don't have any fixed infrastructure. Due to the mobility nature of nodes data transmitted from one node to another is not reliable. So it is a challenging task to secure the data transmitted in WSN.

3. Large scale node deployment: Number of nodes in a traditional WSN will be more when compare to Ad-hoc network and also to provide redundancy, density of node deployment increases. For these two reasons security mechanisms also needs to scale as the scale of network increases [2].

Attacks in WSN

Attacks in WSN can be categorized into three categories based on capabilities [5][6].

A. Internal and External attacks: External attack injects unwanted data in to the network for service interruption and raises a Denial of Service attack. Internal attacks raise from the network to interrupt the current process and exploits the network resources.
B. Passive and Active attacks: Passive attacks are difficult to detect because they monitor the network traffic without modifying the content. Here the attacker collects the sensitive data. In the case of active attacks the intruder interrupts the network communication by modifying the data.

March - April 2020
ISSN: 0193-4120 Page No. 10671 - 10677

C. Laptop-class and mote-class attacks: Laptop class attack targets more powerful devices which has more battery power, strong radio transmission and sensitive antenna etc. In mote-class attack the attacker hacks normal network nodes with same capability to hack data from the network.

What is DoS attack?

DoS attack is an external attack. If this attack exists, network resources will not be available to the registered users [7]. Nodes in the network consume more power and degrade the network performance [7]. DoS attacks occur in different layers of wireless sensor network. Attacks created in different layers of sensor network is listed below[8][9]

- Physical layer: Jamming and tampering
- Data Link layer/MAC layer: Collision, exhaustion, unfairness, interrogation and denial of sleep attacks
- Network layer: spoofing, replaying or altering routing traffic, hello floods, selective forwarding and homing.
- Transport layer: SYN flood and desynchronization attack
- Application layer: Overwhelming sensor, Path-based DoS and Deluge attack.

Most common DoS attacks in WSN are selective forwarding and hello flood attack which increase resource scarcity in the network. Many detection schemes are proposed to detect these two attacks in the network. This paper presents a review on various detection mechanisms proposed to detect DoS attacks.

II. DETECTION MECHANISMS

Security is the major challenge in WSN because of its resource constraints, communication limitations and dynamic network topology. Lot of research work is going on nowadays to provide security to WSN using cryptography algorithms. This section discusses different detection methods used in wireless sensor network.

A. Chen et al.(2011)

In this paper a time-division secret key protocol (TDSKP) [10] for WSN is presented to detect jamming attack. Network time protocol server is used for synchronizing time of all sensor nodes. Time duration between time server and sensor node are initially set to bootstrap. Wireless sensor nodes time synchronization process is used to check time server and the exchange of secret key done during this synchronization time. In this protocol encryption and decryption methods are based on a stream cipher.

B. Shah et al. (2014)

Here the authors proposed a light weight authentication algorithm [11] for authenticating sensor nodes. The algorithm has three phases namely initialization phase, authentication at node phase and authentication at base station phase. For encryption a combination of substitution cipher and columnar transposition is used. The protocol works as follows; a secret key is generated using random number generator in the initialization phase.

C. Young et al. (2013)

In 2013 Young et al. introduced a narrative synchronization and authentication approach using authentication masking code [12] for power efficient authentication. This approach is mainly designed for the security vulnerabilities in T-MAC protocol. Along with RTC packet a kind of PN sequence number known as AMC also send to the receiver node. The attacker node cannot get synchronization to respond with CTS packet. So the normal nodes can send CTS packet without any intrusion.

D. Athmani et al. (2017)

Heterogeneous wireless sensor networks have powerful processor, high capacity memory storage and batteries that can cover large communication areas. In [13] the authors proposed a dynamic authentication and key management scheme EDAK to increase the security level. Different phases involved in EDAK key establishment are pre-deployment phase, key generation phase, EDAK node revocation and addition phase and EDAK authentication algorithm. In the first phase the sensor nodes are preloaded with 128 bit length unique key IK. Key generation phase is based on a light weight algorithm. For every communication this algorithm will be executed and a new key will be generated. In EDAK node revocation and addition phase a new light weight authentication algorithm is used to check the identity of the nodes. Here along with each packet an authentication cade is transmitted to protect the data from the intruder.

E. Yi-ying et al. (2012)

In their proposed work the authors presented a message observation mechanism [14] (MoM) to detect and defend DoS attacks in WSN. MoM uses similarity mechanisms to find the malicious node causing content attack and frequency attack. MoM uses two different types of message lists namely normal message list (NML) and abnormal message list (AML) for the identification of fake messages. This mechanism installed in the cluster head (CH). Number of messages and content of the messages are used to detect the attack. If the observation mechanism finds any bogus message the ID of malicious node will be informed to the CH to refuse messages from that node.

F. Gope et al. (2016)

The proposed work mainly focus on WSN based anonymous authentication protocol [15] and has three different phases namely User registration phase, Remedy phase and Re-Loading phase for the detection of DoS attacks. In the first phase all the legal users has to register with Gateway (GW) to get the service. A smart card will be generated by adding a temporary ID (TID), secret key and a set of shadow identities and Emergency keys and kept safe in the database of GW and will be given to the user through secure channel. In remedy phase an authentication request will be given to the GW with a valid TID and the GW validate the message and also generates a new TID and send back to the user. If any intruder attacks or communication error occurs in between then the user cannot receive the updated TID. So a remedy request will be given by the user to get the new TID and a session key. In the Re-Loading phase new set of shadow identities and emergency keys will be loaded after the expiration of old set.

G. Raja and Marsaline (2014)

In 2014, they have proposed an exclusive communication algorithm known as Fiege Fiat Shamir algorithm [16] for the authentication of nodes in WSN. This algorithm is used for the detection and removal of fake nodes. The simulation has been made in NS2 and analyzed over the terms like network packet delivery ratio and throughput. They have applied this algorithm for health care monitoring system to provide authenticated access to number of patients.

H. Rathore and Hussain (2015)

In their proposed work they have suggested a light weight, efficient, dynamic and secure authentication protocol [17] for authenticating sensor nodes. The proposed protocol has two phases: registration phase and authentication phase. In the first phase encrypted token generation request will be given by the sensor node to the base station. Base station decrypts the message and generates a token for the sensor

node. The generated token along with incremented nonce is sent back to the node. The sensor node decrypts the nonce with its secret key to check the base station. If decryption is successful then the token is added in the database of the node. In the authentication phase all the nodes mutually authenticate each other with the help of their tokens.

Table: 1. Features and challenges of detection mechanisms

Author [citation]	**Methodology**	**Features**	**Challenges**
Chen et al. [10]	Time-division secret key protocol	• This scheme manages nodes effectively. • Reduce unnecessary energy consumption	• Mobility of nodes not considered
Shah et al. [11]	Light weight authentication algorithm	• Suitable for secure group communication • High scalability • Processing overhead minimized. • Memory usage minimized	• Lack of real time response
Young et al. [12]	Authentication masking code	• Provides synchronization and authentication simultaneously.	• Care should be taken while synchronization or else more errors will occur. • Design of dynamic AMC allocation algorithm is crucial.
Athmani et al. [13]	Dynamic authentication and key management scheme	• Improves energy efficiency • Use pre-existing information to generate dynamic keys • Flexible and scalable	• Don't address data integrity and freshness
Yi-ying et al.[14]	Message observation mechanism	• Use spatiotemporal correlation • Reduce energy consumption	• Mobility and location information not added
Gope et al. [15]	Anonymous user authentication protocol.	• Can be added with existing protocols • Reduce computational and communication overhead during resynchronization process	• Complex when severity exceeds.
Raja and Marsaline [16]	Fiege Fiat Shamir algorithm	• Can be used in real time application • High throughput • High packet delivery ratio	• Care should be taken while malicious node elimination
Rathore and	Simple, dynamic , light	• Can be implemented in real time	• Not suitable for

Hussain [17]	weight and secure authentication protocol	WSN • Decreases storage and communication overhead	detecting potential attacks.

III CONCLUSION

Due to limited resources, providing data security to WSN is one of the major challenges faced by many real time applications. In this paper we have discussed few detection mechanisms used for detecting DoS attacks in the WSN. Different algorithms were studied and the features and challenges were identified. From the analysis it is identified that some of the detection mechanisms doesn't consider mobility of the node and some are not suitable for real time applications. Most of the algorithms reduces computational complexity and storage usage and improves energy efficiency.

REFERENCES

[1].Yong wang, GarhanAttebury and ByravRamamurthi, "A survey of security issues in wireless sensor network," IEEE Communications Curveys& Tutorials, Vol.8, no.2, pp. 1-22.

[2] Elaine Shi and Adrian Perrig, "Designing Secure Sensor Networks", IEEE wireless communications, vol. 11. no 6, pp 38- 43.

[3] Joyashree Bag, Subhashis Roy, Subir Kumar and Sarkar," (2014) Realization of a Low Power Sensor node Processor for Wireless Sensor Networks and its VLSI Implementation", IEEE International Advance Computing Conference (IACC), pp 101 -105.

[4] Qian Zhao, YukikazuNakamoto and ZulfazliHussin, (2013) "Energy- Efficient Protocol for Extending Battery Life in Wireless Sensor Network" ,IEEE 33rd International Conference on Distributed Computing Systems Workshops, pp 268-273.

[5] Parli B. Hari and Shailendra Narayan Singh, (2016) "Security Issues in Wireless Sensor Networks: Current Research and Challenges", International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring).

[6].Jitender Grover and Shikha Sharma, (2016) "Security Issues in Wireless Sensor Network-A Review", 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp 397-404.

[7] AshishPatila and Rahul Gaikwad, "Comparative Analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Networks", Procedia Computer Science, vol. 48,pp. 387-393.

[8] David R. Raymond and Scott F. Midkiff, "Denial-of-service in Wireless Sensor Networks: Attacks and Defenses", Pervasive Computing, vol. 7, no. 1, pp 74-81.

[9] Opeyemi A. Osanaiye , Attahiru S. Alfa and Gerhard P. Hancke, "Denial of Service (DoS) Defence for Resource Availability Wireless Sensor Network", IEEE Access, vol.6, 6975-7004.

[10] J. Chen, Y. Ma, X. Wang, Y. Huang and Y. Lai, (2011) "Time-division secret key protocol for wireless sensor networking," IET Communications, vol. 5, no. 12, pp. 1720-1726.

[11] Manali D. Shah, Shrenik N. Gala and Narendra M. Shekokar, (2014) "Lightweight Authentication protocol used in Wireless

Sensor Network", International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp 138- 143.

[12] Young-ho Son, Jin-keun Hong and Keun-sung Bae, "Authentication masking code against DoS of T-MAC Protocol", Springer, pp 1889–1895.

[13] SamirAthmani, AzeddineBilami and DjallelEddineBoubicheEDAK: An Efficient Dynamic Authentication and Key Management Mechanism for Heterogeneous WSNs", Future Generation Computer Systems, vol. 92, pp 789-799.

[14] ZHANG Yi-ying LI Xiang-zhen and LIU Yuan-an, "The Detection and Defence of DoS Attack for Wireless Sensor Network", The Journal of China Universities of Posts and Telecommunications, vol 19, pp 52–56.

[15] P. Gope, J. Lee and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," IEEE Sensors Journal, vol. 17, no. 2, pp. 498-503, 15.

[16] K. Nirmal Raja and M. MarsalineBeno, "On Securing Wireless Sensor Network- Novel authentication scheme against DOS attacks", Journal of Medical Systems, vol. 38, pp. 1-5.

[17]. R. Rathore and M. Hussain, "Simple, secure, efficient, lightweight and token based protocol for mutual authentication in wireless sensor networks", in Emerging Research in Computing, Information, Communication and Applications, Springer India, 2015, pp. 451-62.