International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

DDoS Attack Detection and Prevention on Wireless Sensor Network by Using TBT Method

Ms. Riya soni[1], Mr. Rajneesh Pachouri[2], Mr. Anurag Jain[3]

[1]M.Tech Research Scholar Department of Computer Science Engineering AIST, Sagar
[2,3]Assistant Professor,Department of Computer Science Engineering AIST, Sagar

---

Abstract - *Managing DDoS attacks on WSNs is becoming increasingly complex, and it has reached a point where it is difficult to see Zombies spread across the network. On the other hand, this hinders the understanding of the DDoS status. The variety of known attacks creates the impression that the problem area is large, and it is difficult to diagnose and deal with it. In order to differentiate attacks and protect researchers need to better understand the problem and the current solution environment. The process of planning an attack on WSNS is very complicated. After analyzing the existing frameworks, we have identified three types of DDOS frameworks: victim protection frameworks, resource protection frameworks, and distributed security frameworks. It is too late for victim protection agencies to respond to DDOS attacks. Source protection framework is unable to achieve optimal performance due to lack of attack data. Conversely, a distributed framework can achieve better co-operation between multiple distributed security systems. We suggest retrieval mechanisms to control unwanted traffic by reducing DDOS-based flood attacks. The function focuses mainly on the detection algorithm should detect DDOS attacks from a source that comes from high reliability by using Trace Back Technique (TBT).*

Key Words: **DDos, TBT, Attack, WSN, Security**

1.INTRODUCTION

Recent advances in wireless and digital electronics have enabled the creation of low-cost, low-power, multifunctional nodes in small sizes and uninterrupted connections in short distances. These small sensor nodes, which contain sensors, data processing, and communication materials, add meaning to sensory networks depending on the concerted effort of a large number of nodes. Sensitive networks show significant improvements than traditional sensors, which are used in the following two ways:

Sensors can be placed away from real action, that is, something known from the perception of the mind. In this approach, large sensors that use certain complex techniques to separate targets from natural noise are required.

• Only several sensors can be used. The sensory positions and communication structures are carefully designed. They transmit a series of action times that are heard in the central nodes where the calculations are performed and data is included.

• The sensor network is made up of a large number of sensor nodes, which are widely distributed within or near the event.

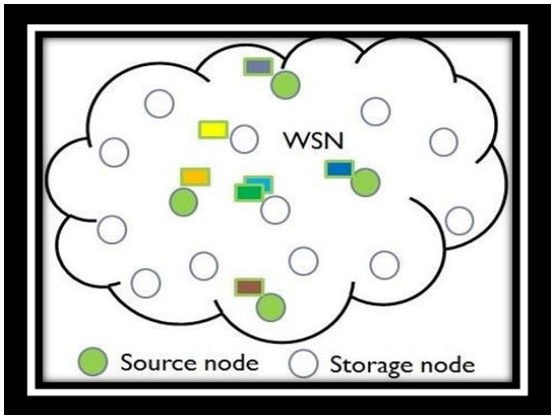

Fig 1: An Example visualization of Wireless sensor network

1.1 Sensor Networks Communication Architecture

Nerve nodes are usually distributed in the sensory field as shown in Fig. 1.2. Each of these scattered nerve components has the ability to collect data and route data back to the sink and end users. Data is returned to the end user by multi-hop infrastructure under-sink construction as shown in Fig. 1.2. The sink can connect to the task manager node via Internet or Satellite.

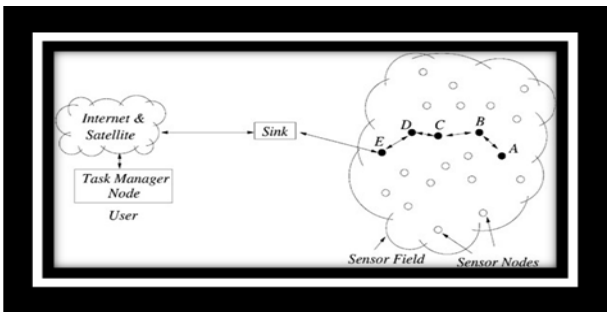

Fig. 2: Sensor nodes scattered in a sensor field

This protocol stack combines power and route awareness, integrates data and communication processes, connects power efficiently via wireless medium, and promotes collaborative efforts of sensor nodes. Protocol stack contains application layer, transport layer, network layer, data link layer, Physical layer, power management plane, motion management plane, and task management plane.

1.2 Security in WSN

Wireless network applications include marine and wildlife monitoring, equipment operation, building safety and earthquake monitoring, and many military applications. A wide range of future applications are likely to follow, including highway rentals, land pollution, wildfires, security construction, water quality, and human heartbeat. The main advantage of these programs is that they enable internal processing to reduce large streams of raw data into useful integrated data. Protecting everything is important. Because sensory networks present different challenges, the traditional security strategies used in traditional networks cannot be applied directly. First, to make sensory networks economically viable, sensory devices are limited in their power, integration and communication functionality. Second, unlike traditional networks, sensor nodes are often installed in accessible areas, presenting an increased risk of physical attack. Third, sensory networks interact more closely with their physical locations and people, introducing new security concerns. As a result, existing security measures are inadequate, and new ideas are needed. Fortunately, the new challenges also encourage new research and represent an opportunity to better address network security from the outset.

2. LITERATURE SURVEY

1. **Saman Taghavi, James Joshi 2013** [1] Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals. DDoS flood attacks are a clear attempt to disrupt official users' access to services. Attackers often gain a large number of computers by exploiting their vulnerability to set up invading armies (i.e., Botnets). Once an attack force has been established, the attacker may request a systematic attack, targeting one or more targets. Creating a comprehensive defense against DDoS floods identified and anticipated is a desirable goal for the research community for detection and prevention. However, the implementation of such an approach requires a thorough understanding of the problem and the techniques used to date in preventing, detecting and responding to various DDoS flood attacks. In this paper, they assess the magnitude of the DDoS flood problem and try to combat it. We classify DDoS flood attacks and plan existing strategies based on where, when, and how they protect against DDoS flood attacks. In addition, they highlight the need for a comprehensive approach to distribution and cooperation. Our main objective in this project is to inspire the research community to develop effective, efficient, and comprehensive prevention, recovery, and response systems that address the DDoS flood problem before, during and after actual attacks.
2. **Pelechrinis, Konstantinos, Marios Iliofotou 2011** [2] The shared nature of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack. Recent studies, however, indicate that such attacks can be easily accomplished using off-the-shelf machines. To give a simple example, a malicious node can continue to transmit a radio signal to block any official access to the medium and / or to interrupt reception. This action is called jamming and malicious nodes are called jammers. Jamming techniques vary from simple depending on the continuous transmission of disturbance signals, to complex attacks aimed at exploiting the risk of a particular process used. In this study, they present a detailed timely discussion of the jamming attacks recorded in the literature.
3. **Yan, Qiao, F. Richard Yu, Qingxiang Gong2016** [3] Distributed Denial of Service (DDoS) attacks in cloud computing environments are growing due to the essential characteristics of cloud computing. With the latest developments in software-defined (SDN) network, SDN-based cloud brings new opportunities to overcome DDoS attacks in cloud computing environments. However, there is a controversial relationship between SDN attacks and DDoS. On the other hand, the power of SDN, including traffic-based software analysis, centralized control, global network viewing, dynamic update of transmission rules, makes it easier to detect and respond to DDoS attacks. On the other hand, the security of the SDN itself is still being improved, and the existing DDoS vulnerabilities can exist across all SDN platforms. In this paper, they discuss new trends and features of DDoS attacks in cloud computing, and provide an in-depth study of ways to protect against DDoS attacks using SDN.
4. **Latif, Rabia, Haider Abbas, and Saïd Assar2014** [5] Wireless Body Area Networks (WBANs) have emerged as a promising technology that has shown enormous potential in improving the quality of healthcare, and has thus found a broad range of medical applications from ubiquitous health monitoring to emergency medical response systems. A large amount of sensitive data collected and processed by WBAN nodes requires advanced and secure processing infrastructure. Given the limited resources of WBAN storage and storage facilities, the integration of WBANs with computer computing can provide a powerful solution. However, apart from the benefits of cloud-based WBAN, several security issues and challenges remain. Among these, data access is a major security issue. The biggest threat to data acquisition is a service-sharing (DDoS) attack that directly affects the regular availability of patient data.
5. **Shamshirband, Shahaboddin 2014** [8] Owing to the distributed nature of denial-of-service attacks, it is tremendously challenging to detect such malicious behavior using traditional intrusion detection systems in Wireless Sensor Networks (WSNs In the present paper, a game theory approach, which is a cooperative Game-based Fuzzy Q-learning (G-FQL), is introduced. G-FQL uses a combination of both game-based theoretic

approach and a non-compliant Q-learning algorithm at WSN. It is a three-player strategy game consisting of sink nodes, a base station, and an attacker. The game performs whenever a network victim receives a flood package such as a DDoS attack across a certain border of the WSN alarm event. The proposed model uses co-operative attack conditions for sink attack and a base station to act as rational players who make decisions through game theory strategy.

3. METHODOLOGY

1. Denial of Service in Sensor Networks

We propose a new IP traceback process that differs in packet marking and is based on TTL identification. This approach was initially proposed for IPv4 networks.
Various IP return methods have been suggested so far. Some of them are compatible with existing infrastructure and some need to be modified, but the effectiveness of any reversal process can be measured by the following factors.

1. Capability of tracing any type of DoS attack.
2. Minimum overhead in terms of storage requirements.
3. Minimum processing requirements on the routers.
4. Least complexity in path reconstruction algorithm (if any).
5. Faster convergence.

This hybrid technique was proposed by taking into account all the above mentioned characteristics.

The aim of all the traceback techniques is to identify the sources of attacking traffic but path reconstruction algorithms actually reveal the identity of first router on the path. The best way would be to get an algorithm that identifies the identity of the original router without requiring the participation of all routers on the way.

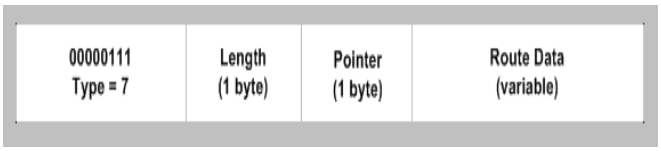

Figure 3: Record Route Option

The problem of source address spoofing can be solved by a technique called Ingress Filtering in which the router discards the incoming packets with invalid source IP address. A serious limitation of this technique arises when the attacker forges the address to the one that belongs to the same network as the attacker's host. Ingress filtering is commonly done at the border router. So, this technique is not effective for internal attacks.

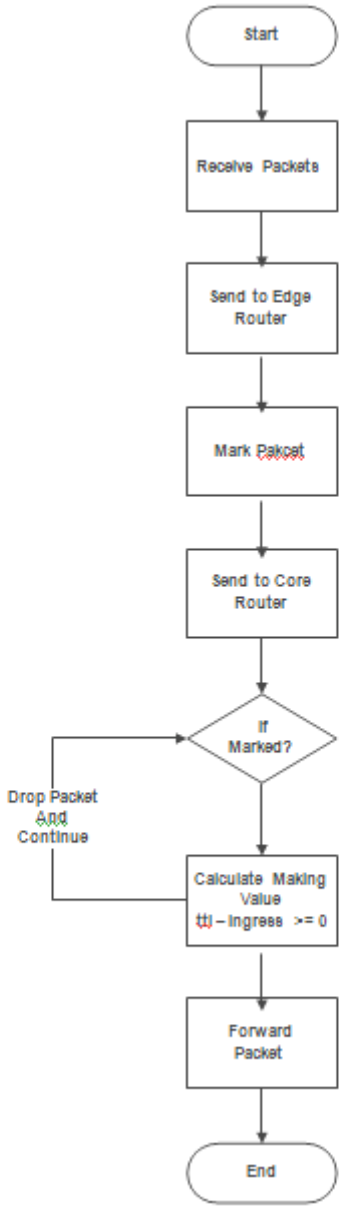

Figure 4: Flow Chart for the proposed IP traceback technique

4. RESULTS AND DISCUSSION

In this section, we analyze the effect of various preventive measures and show that our proposed approach is better than the existing defense method.

Table 1 and Figure 5 show the effect of the proposed cleaning method on the input with a different number of invaders. This figure indicates that the proposed protection mechanism (Disabling IP Broadcast) greatly reduces the effect of DDoS-based flood attacks on a large scale. Table 5.4 and Figure 6 show the impact of the proposed prevention strategies on the Number of Conflicts with a different number of attackers and show a comparison of the existing defense system. This figure indicates that the proposed protection mechanism (Disabling IP Broadcast) greatly reduces the effect of DDoS-based flood attacks on a large scale. By using this The number of collision strategies decreases compared to the collision of an existing defense system.

Table 1 Effect of Proposed Prevention Technique on Throughput with varying number of attackers

Attackers	Throughput
1	1714653
2	1617242
3	1530967

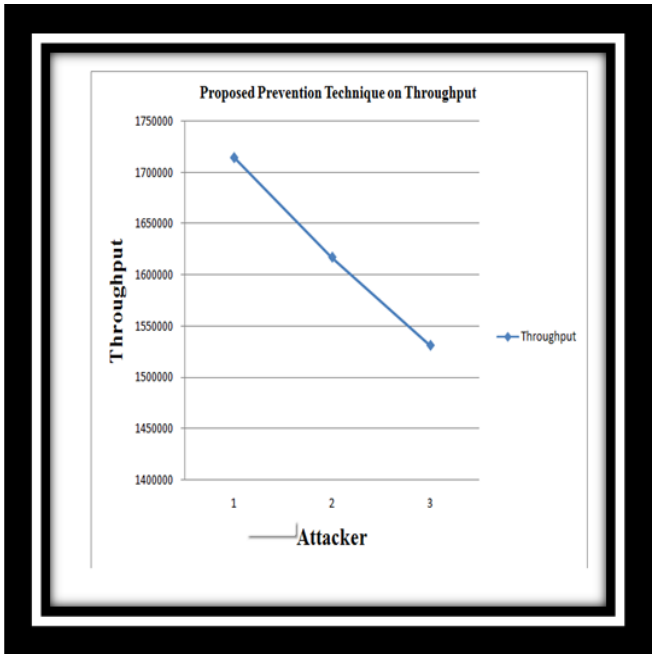

Figure 5: Effect of Proposed Prevention Technique on Throughput with varying number of attackers

Table 2 Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

Attackers	Existing	Proposed
1	3955	2630
2	4018	2740
3	4175	2795
4	4210	2835
5	4315	2952

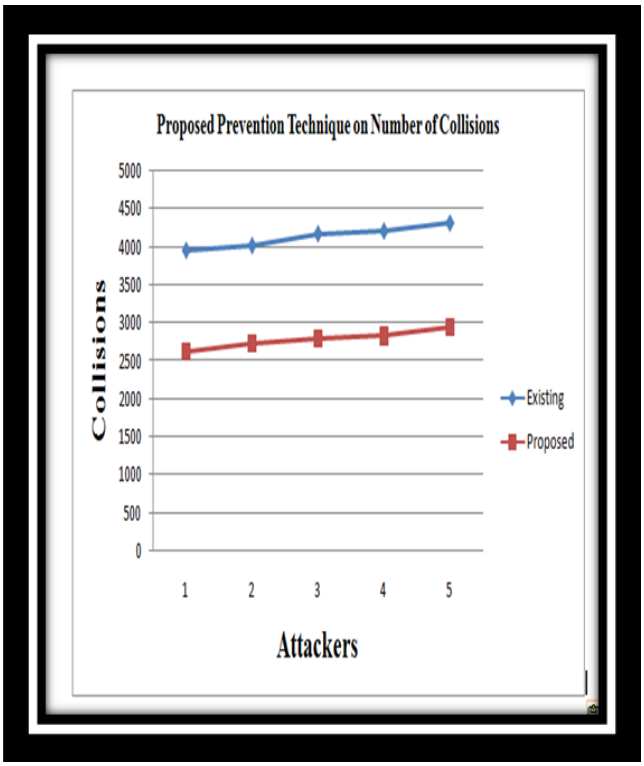

Figure 6: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers

5. CONCLUSION AND FUTURE SCOPE

This work has been used to mimic the enlightenment that the way can get attackers in a short time. DDoS security systems can be used on the network to detect DDoS attacks independently for example, IDS but these processes often fail to detect the attacker himself. Life time of the field. Lifetime (TTL) or hop limit is a method that limits the life or life time of data on a computer or network. TTL can be started as a counter or time stamp attached or embedded in the data. When the specified event number or duration has elapsed, the data is discarded. In computer communication, TTL prevents the data packet from circulating indefinitely. The purpose of this study was to control unwanted traffic by

reducing DDOS flood-related attacks using IP Traceback. The IP Traceback algorithm has been able to detect DDOS attacks from a source that comes from high reliability. The security framework operates in a distributed network mode. The DDoS response process tries to filter out most attack packets without compromising the quality of the user / actual traffic.

DOS attacks attempt to eliminate and eliminate the victim's bandwidth or server capacity. In a DDOS attack, the attacker threatens a large number of cybercriminals and orders them to carry out organized attacks. This study has made progress in preventing or at least greatly reducing the impact of various security risks, real progress in the fight against DDOS is still lacking. In the future, we would like to work on implementing Trace back strategies in IPv6 environments another direction for future work could be to improve DNS-related detection performance and other spoof-related threats. Improving the acquisition performance is researching the proposed program with many other Traceback strategies. Much work is needed to stem the tide of bandwidth threats where it is almost impossible to launch memory attacks against computer-generated DCs.

REFERENCES

[1] Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." *IEEE communications surveys & tutorials* 15, no. 4 (2013): 2046-2069.

[2] Pelechrinis, Konstantinos, Marios Iliofotou, and Srikanth V. Krishnamurthy. "Denial of service attacks in wireless networks: The case of jammers." *IEEE Communications Surveys & Tutorials* 13, no. 2 (2011): 245-257.

[3] Yan, Qiao, F. Richard Yu, Qingxiang Gong, and Jianqiang Li. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges." *IEEE Communications Surveys & Tutorials* 18, no. 1 (2016): 602-622.

[4] Huang, Qiang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, and Jinyun Zhang. "Fast authenticated key establishment protocols for self-organizing sensor networks." In *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pp. 141-150. ACM, 2003.

[5] Latif, Rabia, Haider Abbas, and Saïd Assar. "Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review." *Journal of medical systems* 38, no. 11 (2014): 128.

[6] Lupu, Teodor-Grigore, I. Rudas, M. Demiralp, and N. Mastorakis. "Main types of attacks in wireless sensor networks." In *WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering*, no. 9. WSEAS, 2009.

[7] Gill, Khusvinder, and Shuang-Hua Yang. "A scheme for preventing denial of service attacks on wireless sensor networks." In *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE*, pp. 2603-2609. IEEE, 2009.

[8] Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.

[9] Yu, Yanli, Keqiu Li, Wanlei Zhou, and Ping Li. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." *Journal of Network and computer Applications* 35, no. 3 (2012): 867-880.

[10] Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh. "Overview of security issues in wireless sensor networks." In *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*, pp. 308-311. IEEE, 2011.

[11] Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.

[12] Arunmozhi, S. A., and Y. Venkataramani. "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks." *arXiv preprint arXiv:1106.1287* (2011). [13] Nanda, Rohan, and P. Venkata Krishna. "Mitigating denial of service attacks in hierarchical wireless sensor networks." *Network security* 2011, no. 10 (2011): 14-18.

[14] Jan, Mian, Priyadarsi Nanda, Muhammad Usman, and Xiangjian He. "PAWN: a payload-based mutual authentication scheme for wireless sensor networks." *Concurrency and Computation: Practice and Experience* (2016).

[15] ELBeltagy, Maha, Sarah Mustafa, Jariya Umka, Laura Lyons, Ahmed Salman, Chur- Yoe Gloria Tu, Nikita Bhalla, Geoffrey Bennett, and Peter M. Wigmore. "Fluoxetine improves the memory deficits caused by the chemotherapy agent 5- fluorouracil." *Behavioural brain research* 208, no. 1 (2010): 112-117.

[16] Misra, Sudip, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena, and Mohammad S. Obaidat. "A learning automata based solution for preventing distributed denial of service in Internet of things." In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, pp. 114-122. IEEE, 2011.

[17] Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.

[18] Kumar, P. Arun Raj, and S. Selvakumar. "Detection of distributed denial of service attacks using an ensemble of

adaptive and hybrid neuro-fuzzy systems." *Computer Communications* 36, no. 3 (2013): 303-319.
[19] Baig, Zubair A. "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks." *Computer Communications* 34, no. 3 (2011): 468-484. [20] Li, Shancang, Lida Xu, Xinheng Wang, and Jue Wang. "Integration of hybrid wireless networks in cloud services oriented enterprise information systems." *Enterprise Information Systems* 6, no. 2 (2012): 165-187.
[20] Li, Shancang, Lida Xu, Xinheng Wang, and Jue Wang. "Integration of hybrid wireless networks in cloud services oriented enterprise information systems." *Enterprise Information Systems* 6, no. 2 (2012): 165-187.
[21] Ho, Jun-Won, Matthew Wright, and Sajal K. Das. "Distributed detection of mobile malicious node attacks in wireless sensor networks." *Ad Hoc Networks* 10, no. 3 (2012): 512-523.
[22] Hamdi, Mohamed, and Noureddine Boudriga. "Detecting Denial-of-Service attacks using the wavelet transform." *Computer Communications* 30, no. 16 (2007): 3203- 3213.
[23] Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." *Ad Hoc Networks* 9, no. 5 (2011): 727-735.
[24] Vasserman, Eugene Y., and Nicholas Hopper. "Vampire attacks: draining life from wireless ad hoc sensor networks." *IEEE transactions on mobile computing* 12, no. 2 (2013): 318-332.
[25] Redwan, Hassen, and Ki-Hyung Kim. "Survey of security requirements, attacks and network integration in wireless mesh networks." In *New Technologies, Mobility and Security, 2008. NTMS'08.*, pp. 1-5. IEEE, 2008.