EAI Endorsed Transactions
on Energy Web and Information Technologies
Research Article EAI.EU

An Efficient Routing Approach for Detection of Syn Flooding Attacks in Wireless Sensor Networks

Dr.T. Sasilatha[1,*], S.Balaji[2], Dr.P.Suresh Mohan Kumar[3]

[1]Dean, Department of EEE, AMET Deemed to be University, Chennai, Tamilnadu, INDIA – 603112.
[2]Asst.Prof, CSE Department, Panimalar Engineering College, Chennai, Tamilnadu, INDIA – 600123.
[3]Professor and Dean, DMI College of Engineering, Chennai, Tamilnadu, INDIA – 600123.

E-Mail: sasi_saha@yahoo.com, balajiit@gmail.com, psureshmohankumar@gmail.com

Abstract

In wireless environment researches on security issues in various layering level of the networks are focused recent times. One of the major issue is denial of service attacks. This paper mainly deals with the detection of syn flooding attacks which is one form of denial of service attacks in wireless sensor networks. It is a type of attack done by the attacker to a specific server to down them by flooding the requests. So, the server will be busy waiting for the requests created by the attacker. In view to this attack an efficient routing approach by distance-2 dominating set is proposed to exhibit the plan of clustering the nodes in the network for effective data transmission. The traffic limit method is used to monitor the bandwidth usage of the nodes concerned in the network to find the flooding attacks in real time event detection environment. The test cases are implemented using network simulation tool. The outcomes discussed about here are to demonstrate the packet delivery ratio, end-to-end delay and the bandwidth usage by the malicious nodes which will be high of the various other authorized nodes in the system.

Keywords: Network security, denial of service, syn flooding, domination set, wireless sensor networks.

Received on 07 May 2018, accepted on 07 July 2018, published on 12 September 2018

3rd International Conference on Green, Intelligent Computing and Communication Systems - ICGICCS 2018, 18.5 - 19.5.2018, Hindusthan College of Engineering and Technology, India

doi: 10.4108/eai.12-9-2018.155562

1. Introduction

Wireless sensor networks guarantee energizing new applications in the near future, for example, consistent network, ubiquitous on-demand computing power and deployable communication required in a first responders and military purposes. These systems as of now screen production line execution, ecological conditions to give some examples applications. There are some attacks that can be classified in wireless sensor networks in the layer level such as blackole, deprivation of sleep, loop of routing and denial of service attacks Because of their association, these systems are especially vulnerable against Denial of Service (DoS) attacks many research works has been done to improve survivability. The classification of syn flooding attacks is one of the major issues in denial of service attacks(S.Kandula et.al 2005).

Here, we think about how routing protocols however intended to be secure, need assurance from these attacks which exhaust life from these systems. There are three essential commitments. In the first place, we assess the vulnerabilities of existing protocols completely to routing layer battery depletion attacks. Second we observe that safety efforts to keep these exhaustion attacks are orthogonal to those which are utilized to ensure existing secure directing conventions, and its infrastructure (D.Dagon et.al 2006).Firewalls, like other hardware and software device have vulnerabilities which can be exploited by motivated attackers. Firewalls protect a trusted network from an untrusted network by filtering traffic according to a specified security policy. A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the internet.

*Corresponding author. Email: sasi_saha@yahoo.com

There are many wireless based protocols used for routing behaviour such as AODV, DSR, and DSDV etc. The routing behaviour of existing and proposed work is analysed using AODV protocol. Here, the domination concept is taken where all graphs assumed are undirected, connected and non-trivial without multiple edges or loops. A set of vertices 'D' in graph 'G' is considered as a dominating set, if each vertex in V–D is closest to some vertex in set D. Domination of graphs has been extensively researched branch of graph theory. Graph theory is one of the most flourishing branches of mathematics and computer applications .

1.1 Basic Scenario

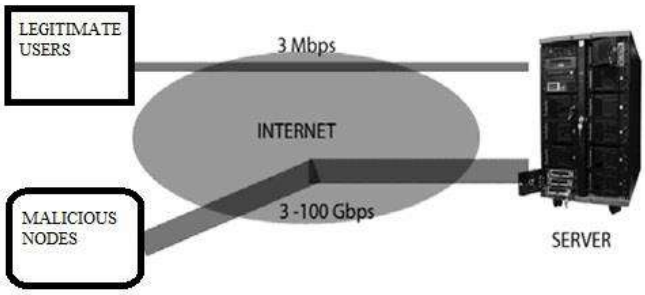

Figure 1. Basic Scenario of syn flooding

Considering the typical scenario under DoS attack especially syn flooding where legitimate users use only a bandwidth of 3 Mbps while the malicious can generate traffic of attack size ranging from 3-100Gbps. Due to this effect the servers get down.

1.2 Types of security attacks on wireless sensor networks

LAYERS	ATTACKS
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption
Datalink layer	Traffic analysis, monitoring and disruption
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Table 1: Attacks Classification in various layers.

The table 1 shown here emphasizes on various attacks occur in network model. The proposed work focuses on the transport layer since it deals with the syn flooding attacks. In this the attacker uses the three-way handshake protocol for the reason of performing the denial of service attack. For understanding this attack first, we need to know about the three-way handshake protocol. First the user will send the TCP SYN request to the server. Now the server will return the TCP ACK for the request. Now user needs to give back the response for the acknowledgment. The three-way handshake protocol is clearly shown in the figure 2.

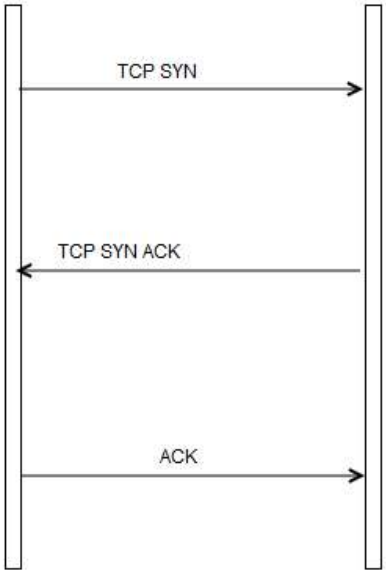

Figure. 2 TCP three-way handshake protocol

The attacker will continuously send the TCP SYN to the server or the target. It returns the acknowledgment to every single attacker's request. But the attacker will not end the protocol. So, the new service needs to wait for response or service. The working of the TCP SYN flood is shown in the figure 3.

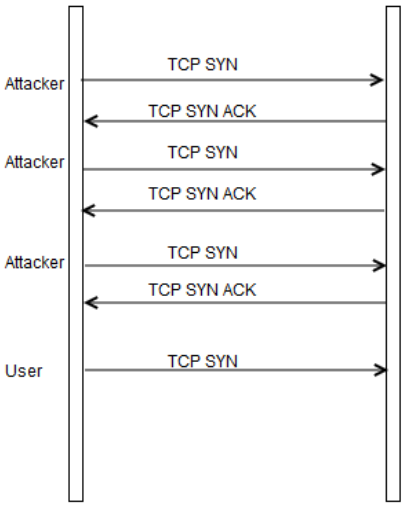

Figure. 3 TCP syn flood

2. Related Works

Security becomes one of the real concerns when there are potential attacks against sensor systems. Numerous administrations in security, for example, validation and key administration, are basic to guarantee the typical tasks of a sensor organize in diverse applications and situations. A.A.Boudhir et.al 2010 study the significant points in WSNs security, and present the primary arrangements in the sensor security, order a large number of the present attacks, We likewise also discuss the proposition design in view of multi operator stage for guaranteeing robust security, without key administration , in remote sensor systems with lower energy consumption. The main disadvantage here is it has no platform implementation, then to evaluate the energy consumption of the proposal platform with solutions based on cryptography.

Pawani porambage et.al 2015 Investigates on the multicast communication protocols by developing group key establishment protocols among the resource constrained devices. However, these devices may not provide better performance results in offline mode.

Islam Hegazy et.al 2010 acquaints lightweight IDS with recognize interface quality attacks on MintRoute in WSNs. The IDS does not require collaboration between the nodes and does not include any correspondence overhead. Also, it upgrades the capacity of the sensor nodes to identify malicious behaviour without requiring particular hardware. Indeed, impulsive utilization of the approach is ineffectual, since an attacker can without much of a stretch distinguish the trick and adjusts its methodology.

3. Efficient Routing Approach by Distance -2 dominating set

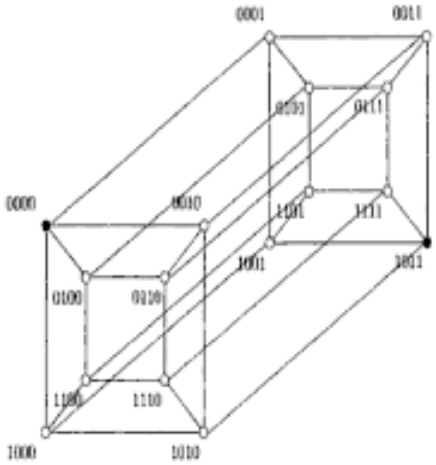

Figure. 4 Distance-2 dominating set in hypercube network

Consider a computer network modeled by a graph G = (V,E),for which vertices represents computers and edges represent direct links between pairs of computers. Let the vertices in following figure represent an array, or network, of 16 computers, or nodes. Each node to which it is directly connected, assume that from time to time we need to collect information from all nodes. We do this by having each node route its information to one of a small set of collecting nodes (a dominating set). Since this must be done relatively fast, we cannot route this information over too long path. Thus we identify a small set of nodes which are close to all other nodes. Let us say that we will tolerate at most a two unit delay between the time a node sends its information and the time it arrives at a nearby collecting node. In this case we seek a distance-2 dominating set among the set of all nodes. The two shaded vertices form a distance-2dominating set in the hypercube network in figure 4.

This description of command communication means that, in terms of command forwarding, the proposed approach has an undirected graph topology. A data could pass via the links in both directions. If the size of the attacker peer list is high, then this design makes sure that each node has at least venues to receive data packets.

3.1 Routing path selection

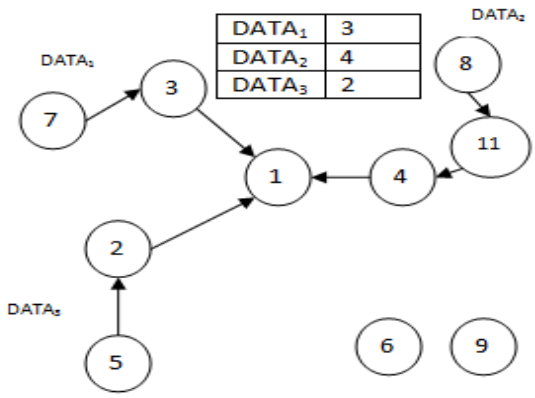

Figure. 5 Routing path selection

The figure 5 shows the route selection of the nodes to transmit the data as per the proposed distance2-dominating set. The nodes are clustered in the network based on the two unit delay tolerant level to make efficient data transmission .The routing information is stored as in the form of routing table which consists of the parameters such as DATA and the node number.

3.1.1 Traffic rate limiting method for syn flooding attacks

This method can be implemented only with the cooperation of the ISP. The organization will limit the bandwidth for the unauthorized request and the regulated traffic will process normally. The drop scenario is presented due to high bandwidth usage in figure 6.

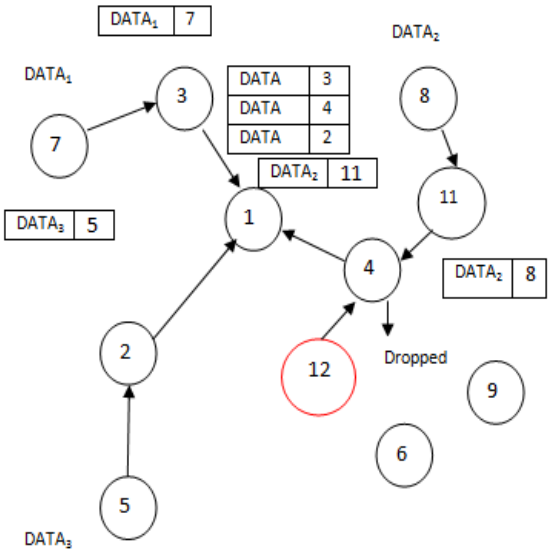

Figure. 6 packet drop scenario by syn flooding attacks

4. Implementation and Results

NS-2 simulation test system is utilized for the usage of the proposed plan. The AODV protocol is used for data transmission. TCP packets were utilized as the alternate. Activity sources utilized are Constant-Bit-Rate (CBR) and the field arrangement is 800 x 800m with 500 nodes. The packet size is taken as 1024 bits at arrival interval rate of 10sec.

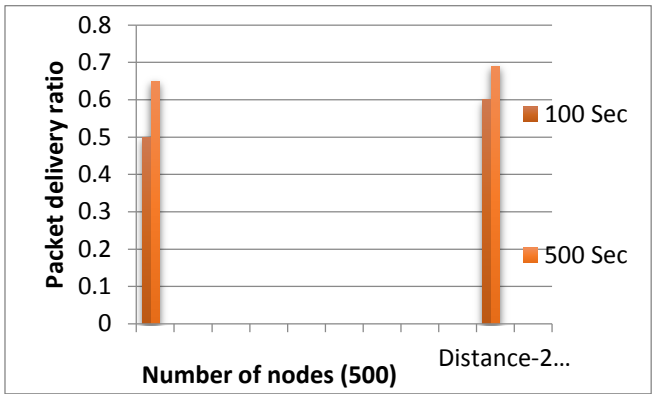

Figure. 7 Comparison of packet delivery ratio for 500 nodes.

In figure 7 the comparison of packet delivery ratio is showed for existing and proposed work. The results proves that the delivery ratio is high in distance-2 dominating set approach by 0.59, 0.69 for the simulation time of 100,500 sec respectively.

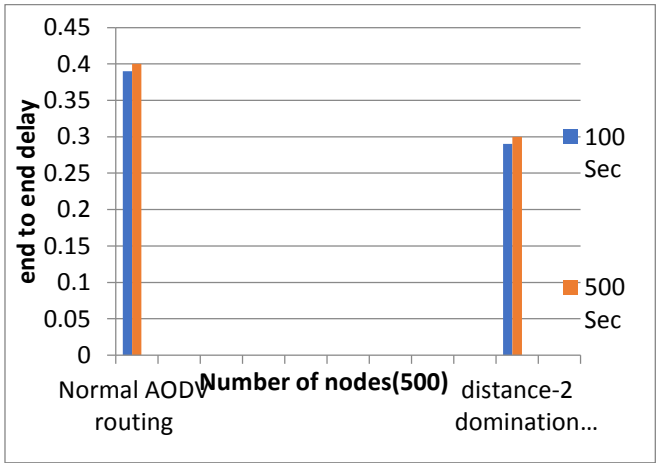

Figure. 8 Comparison of end to end delay for 500 nodes.

In figure 8 the comparison of end to end delay is showed for existing and proposed work. The results proves that the delay is low in distance-2 dominating set approach by 0.27ms, 0.30ms for the simulation time of 100,500 sec respectively.

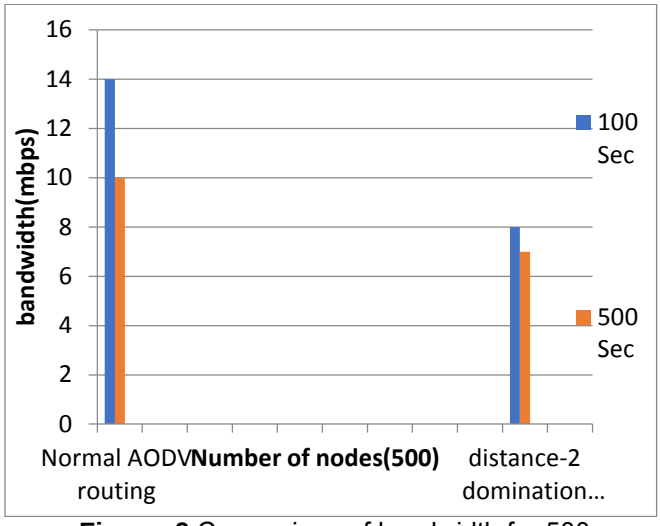

Figure. 9 Comparison of bandwidth for 500 nodes.

The bandwidth usage is within the threshold limit while using the proposed approach whereas in existing approach the cause of this effect by the detection of syn flooding attacks .Hence the bandwidth usage is high than the limit of 8 mbps . The result is shown in figure 9.

5. Conclusion

This work provides the concept on distance-2 dominating set approach for an effective routing to perform data transmission in wireless senor networks. In supporting to this traffic limit method is implemented to monitor the data packets to find out the syn flooding attacks. The evaluation is conducted in a simulation environment for simple networks which has 500 nodes. The analysis of the bandwidth usage, packet delivery ratio and end-to-end delay concludes that the performance is increased up to 20% in proposed work, as compared with the existing approach. In future this approach can be used in mitigating other forms of denial of service attacks.

References

[1] S. Kandula, D. Katabi, M. Jacob, and A. Berger, “Botz-4-Sale: Surviving Organized DDOS Attacks That Mimic Flash Crowds,” Proc. Second Symp. Networked Systems Design and Implementation (NSDI ’05), May 2005.

[2] F. Freiling, T. Holz, and G. Wicherski, “Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of- Service Attacks,” Technical Report AIB-2005-07, CS Dept. RWTH Aachen Univ., Apr. 2005.

[3] D. Dagon, C. Zou, and W. Lee, “Modeling Botnet Propagation Using Time Zones,” Proc. 13th Ann. Network and Distributed System. Security Symp. (NDSS ’06), pp. 235-249, Feb. 2006.

[4] A. Ramachandran, N. Feamster, and D. Dagon, “Revealing Botnet Membership Using DNSBL Counter-Intelligence,” Proc. USENIX Second Workshop Steps to Reducing Unwanted Traffic on the Internet (SRUTI ’06), June 2006.

[5] E. Cooke, F. Jahanian, and D. McPherson, “The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets,” Proc. USENIX Workshop Steps to Reducing Unwanted Traffic on the Internet (SRUTI ’05), July 2005.

[6] N. B. Salem, J.-P. Hubaux, and M. Jakobsson. “Reputation based wi-fi deployment”. *SIGMOBILE Mob. Comput. Commun. Rev.*, 9(3):69–81, 2005.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood ,“The feasibility of launching and detecting jamming attacks in wireless networks”, *MobiHoc ’05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57, Urbana-Champaign (IL), USA, 2005.

[8] Y. Zhang, W. Lee, and Y.-A. Huang, “Intrusion detection techniques for mobile wireless networks”,*Wireless Networks.*

[9] Li Zhao and José G. Delgado-Frias “MARS: Misbehavior Detection in Ad Hoc Networks”, in proceedings of IEEE Conference on Global Telecommunications Conference, November 2007.

[10] A.Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha “Threshold-based Intrusion Detection in Adhoc Networks and Secure AODV” Elsevier Science Publishers B. V., Ad Hoc Networks Journal (ADHOCNET), June 2008.

[11] S.Madhavi and Dr. Tai Hoon Kim “An intrusion detection system in mobile adhoc networks” International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

[12] Afzal, Biswas, Jong-bin Koh, Raza, Gunhee Lee and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks", in proceedings of IEEE Conference on Wireless Communications and Networking, pp.2313-2318, April 2008.

[13] Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar, and Shanmugam, "Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", in proceedings of World Academy Of Science, Engineering And Technology, Vol. 36, pp.1373-1378, December 2008.

[14] Meka, Virendra, and Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks" In Proceedings of the Workshop on Secure Knowledge Management, 2006.

[15] Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp, "A Link Layer Security Protocol for Suburban Ad-Hoc Networks", in proceedings of Australian Telecommunication Networks and Applications Conference, December 2004.

[16] Pawani porambage, An braeken, Corinna schmitt, Andrei gurtov, Mika ylianttila and Burkhard stiller, “Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications”, IEEE Access. Vol 3, pp. 1503-1511, 2015.

[17] A.A.Boudhir , M.Bouhorma and M.Ben ahmed, “Multi-Agents Platform for Security in Wireless Sensor Networks”, International Journal of Computer Science and

Network Security, VOL.10 No.10, October 2010,pp 198-201.

[18] Islam Hegazy,Reihaneh Safavi-Naini, "Towards Securing MintRoute in Wireless Sensor Networks," IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM),2010.

[19] S.Balaji.,T.Sasilatha.,"Detection of denial of service attacks by domination graph application in wireless sensor networks", printed online feb 2018 , Cluster Computing-The Journal of Networks, Software Tools and Applications ,ISSN 1573-7543,Springer.

[20] Mohamed Divan Masood, A.[a],Muthusundar, S.K.[b], "Cryptographic hashing method using for secure and similarity detection in distributed cloud data", Indonesian Journal of Electrical Engineering and Computer Science, Volume 9, Issue 1, January 2018, Pages 107-110

[21] Meenakshi, R.K. , Arivazhagan, A, "RTL modelling for the cipher block chaining mode (CBC) for data security", Indonesian Journal of Electrical Engineering and Computer Science, Volume 8, Issue 3, December 2017, Pages 709-711