Comparison of Variations in Performance of a WSN with Respect to Increasing Node Complexity under DOS Attack and Its Prevention

Shagun Chaudhary[1], **Nitin Kumar**[2]

[1]Jodhpur Institute of Engineering and Technology – School of Engineering and Technology for Girls, Mogra, Jodhpur, Rajasthan, India

Abstract: ***In the recent years, the increase in number of nodes in a typical Wireless Sensor Network has led to specialized applications of these networks which were virtually not possible by the smaller and simpler networks. As the network becomes more complex, the behavior of individual node varies for parameter to parameter. Attacks on network also vary the different network parameters. Detailed analytical study should be employed to study the nature of Wireless Sensor Networks for large number of nodes with respect to different network topologies and different routing protocols along with various types of attacks.***

Keywords: Performance parameters, Packet delivery ratio, Average end to end delay, Denial of service, Node density, Packet drop**.**

1. Introduction

The working of a Wireless Sensor Network is governed and restricted by the number of nodes that form the network. Each individual node has its own geographical range in which it can acquire process and transmit data. With increase in number of nodes the range of different nodes overlap resulting in a complex network. Network efficiency depends on various network parameters like number of packets delivered, number of packets dropped, network throughput and network overhead. Further these parameters are also affected by an attack on the network. The attack hampers the normal working of the network by diminishing available resources [1] [2] [3] [4] [5].

2. Denial of Service Attack & Prevention

A WSN in susceptible to various kinds of attacks ranging from passive eavesdropping to active node disruption and data re-routing [1] [2] [3]. Denial of service is the most common attack on a WSN resulting in diminished resources available for actual data transmission [9] [13] [14]. Dos attack can be isolated or distributed in nature. Also it can occur at every layer of network hierarchy [6][7][8][15]. There are different approaches to detect and prevent a DOS attack but most of them are ineffective mostly due to varied nature of attack as there is large number of possible attack scenarios simultaneously [10][11][12]. We have used the approach of RREQ sequence number detection. Detection and prevention stage is self sustaining and does not require external intervention. The performance of the network recovers effectively after using the prevention algorithm.

3. Simulation Model Parameters

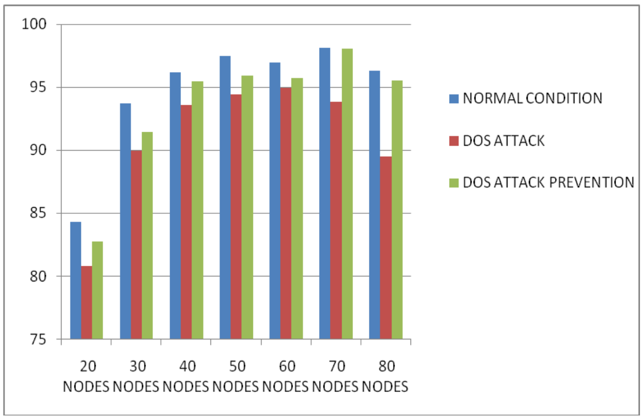
The simulated network consists of 80 nodes and the simulated data is logged in the trace file. The data is further analyzed using awk scripts. The following modeling parameters where considered while network designing and simulation-

Simulator	NS2 (version 2.35)
Simulation Time	200 (s)
Number of Nodes	20, 30,40,50,60,70,80
Simulation Range	1000 × 1000 m
Routing Protocol	AODV
Traffic	CBR
Pause Time	15 (ms)
Max Speed	30 (m/s)
Operating system	Ubuntu-12.04

4. Simulation Data Analysis

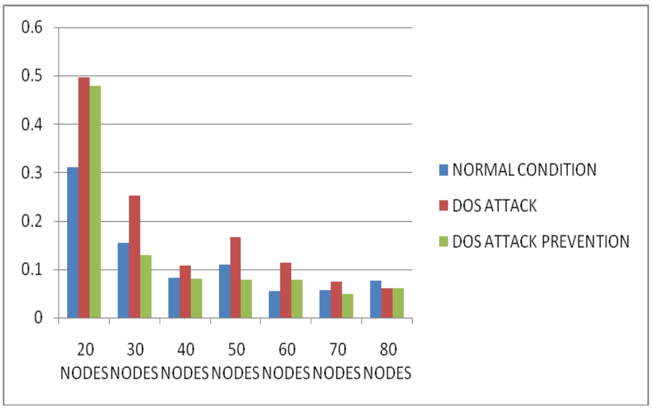
The simulated data is analyzed for four performance parameters defining the network efficiency under no attack condition, under DOS attack and under recovery phase.

4.1 Average Packet Delivery Ratio



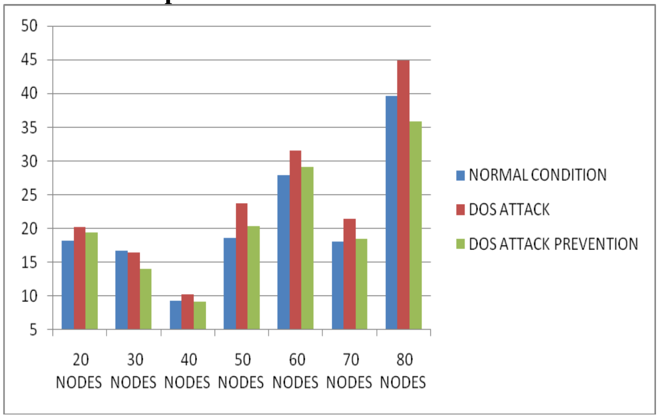
Explanation – The average packet delivery ratio shows variations with respect to increasing node complexity as well as under no attack, attack and attack prevention stages. The packet delivery increases initially with increasing number of nodes as more number of alternate routes are available to data packets but as the network becomes complex, congestion takes toll and packet delivery drops for a network a having large number of nodes. Under attack condition, the packet delivery is reduced for each corresponding node. Under the recovery phase the network tries to deliver maximum packets but the ratio is below the level of corresponding no attack condition.

4.2 End to End Delay



Explanation – Increasing node complexity results in more number of available routes thus shorter paths are always available between sender and receiver leading to corresponding decrease in end to end delays. Under attack the available resources becomes scarce and packet collisions ad network congestion results in increased delays. Under prevention phase, the network returns to its normal working with low delays with increasing number of nodes.

4.3 Packet drop



Explanation – packet drop is directly related to network congestion. As the number of nodes increases initially, alternate routes become available reducing congestion and reducing drop. After a while, network complexity increases to great extent leading to congestion and increased packet drop. Under attack, as the bandwidth and channels becomes restricted, drop increases. Under recovery, the malicious node is removed and network drop reduces.

5. Conclusion

Node complexity defines the range and capabilities of a wireless sensor network. A network having all the resources as bandwidth, memory, power can also become congested if node density is too large. Also DOS attack results in disrupting this resources making the congestion worse. Prevention or recovery schemes can increase the efficiency of the network but cannot restore 100 percent as compared to no attack condition. Thus I can be fairly concluded that the performance parameters fluctuate within a large range with increasing node density and network complexity.

References

[1] Shoo Kumar Singh, M P Singh and D K Singh "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks" International Journal of Computer Trends and Technology - May to June Issue 2011.

[2] Justify Aging Piranha, S. Tephillah and A. M. Balamurugan "Attacks and Countermeasures In WSN" IPASJ International Journal of Electronics & Communication (IIJEC). A Publisher for Research Motivation. Volume 2, Issue 1, January 2014.

[3] Dr. G. Padmavathi and Mrs. D. Shanmugapriy "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[4] S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam "A study of Attacks, Attack detection and Prevention Methods in Proactive and Reactive Routing Protocols" International Business Management 5 (3): 178-183, 2011. ISSN: 1993-5250. Medwell Journals, 2011.

[5] Wassim Znaidi and Marine Minier "An Ontology for Attacks in Wireless Sensor Networks" Jean-Philippe Babau.

[6] Mieso K. Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", Systemics, Cybernetics and Informatics Volume 3 - Number 4.

[7] Anthony D. Wood, John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks," *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, 2004.

[8] Al-Sakib Khan Pathan, "Denial Of Service In Wireless Sensor Networks: Issues And Challenges" Advances in Communications and Media Research, ISBN 978-1-60876-576-8, 2010

[9] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos and Grammati Pantziou, "A Survey on Jamming Attacks and Countermeasures in WSNs" IEEE Communications Surveys & Tutorials, Vol. 11, No. 4, Fourth Quarter 2009.

[10] Marpu Devadas and K.R.Koteeswa Rao, "Security Framework against Denial of Service Attacks In Wireless Mesh Networks" Volume No: 1(2014), Issue No: 10 (October) ISSN No: 2348-4845.

[11] Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta and Neha Garg, "Analysis of Denial of Service (Dos) Attacks In Wireless Sensor Networks", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[12] Farad Amah and Saale K. Das, "Preventing Doss Attacks in Wireless Sensor Networks: A Repeated Game Theory

Approach", International Journal of Network Security, Vol.5, No.2, PP .145–153, Sept. 2007.

[13] Jing Deng, Richard Han, and Shiva ant Dishrag, "Defending against Path-based Doss Attacks in Wireless Sensor Networks".

[14] S. Marti, T. Guile, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM) 2000.

[15] Yi-yang ZHANG, Xiang-Zhen L, Yuan-an LIU, "The detection and defense of Doss attack for wireless sensor network", Elsevier Journal of China Universities of Posts and Telecommunications, Vol. 19, Supplement 2, October 2012

Author Profile

Shagun Chaudhary did her B.tech in 2012 from RTU in Electronics and Communication Engineering. She is currently pursuing M.tech in digital communication from RTU. He is presently working as assistant professor in ECE department in JIET-SETG Jodhpur

Nitin Kumar did his B.tech in 2011 from RTU in Electronics and Communication Engineering. He is currently pursuing M.tech in digital communication from JNU. He is presently working as assistant professor in ECE department in JIET-SETG Jodhpur.