Performance Analysis of Wireless Sensor Networks under adverse scenario of attack

Divya Bharti [a], Neha Nainta [b], Prof. Himanshu Monga [c]

[a] ECE Dept.Final year Engineering student, Jawahar Lal Nehru Govt. Engg. College, Mandi (Himachal Pradesh) (email id- divyabhartikaith@gmail.com)
[b,c] ECE Dept.Final year Engineering student, Jawahar Lal Nehru Govt. Engg. College)

***Abstract*— Wireless Sensor Network (WSN) refers to a group of sensors used for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSN has no mechanism that can organize or check the broadcast of information through the nodes. Nodes themselves are able to transmit the sensed information towards the Base Station, causing greater vulnerability of data being gathered and fiddled with. Amongst many such attacks, Rushing Attack specially is a frequently adapted strategy in On-demand protocol. The counter measure available for such kind of attack is not effective enough as most of the approaches have their own limitations.**

This work focuses on ill effects of Rushing Attack under different conditions with an intend to find out such limitations of each of the earlier adopted counter measures.

Keywords—Wireless Sensor Network, Rushing Attack, Transmission Delay, Packet Delivery Ratio, Infested Node.

I. INTRODUCT ION

At present wireless communication is being widely used and attacks in wireless communication have increased rapidly which causes the data interception and its content is falsified. In wireless communication data transmission depends on the nodes connected to the network so attackers aim a node which carries (transmit) the data in WSN. So it is important to prevent the data from such attacks. Rushing attack takes place in on-demand routing protocol, wherein the infested node rushes the data received from the previous neighbor node and send it as soon as possible to the next neighbor node to establish a path from source to destination.

II. LITERATURE SURVEY

In On-Demand Routing Protocol, a path is established between the sender and receiver, in which a packet is forwarded to discover a path through which data is to be transmitted. To establish a path data is transmitted from one node to the next node. If connection request is received from previous node only, then it will establish the connection with the node and if there already exist the connection request then the request is rejected. First Come First Serve technique is followed in this. Suppose two nodes X and Y both sends the connection request to node Z ,then node Z will establish the connection with the node whose message reaches first and request from the other node is rejected [7]. In Rushing attack infested node aims at rejecting duplicate route discovery messages. The request from the infested node to the next neighboring node for establishing a route is compared to other existing nodes. It can occur in three different locations in between sender and receiver [2][5].

i) Infested node is near the Sender:-

Depicted below are the transmitting terminal and receiving terminal S& R respectively. The .When request for transmission is made , route demand will be established by terminals A & C. It is observed that the infested node A has greater broadcast speed compared to C, hence delivery is made through A and C ,but packet through A will reach the receiver first.

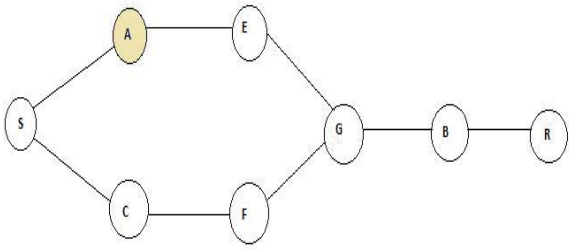

Fig.1: Scenario where attacker is close to the sender.

ii) Infested node is near the receiver node:-

Sender wants to send the route request packet to the receiver. So it will either choose path A, E and G or path C, F and G. B is the infested node and data will be immediately transmitted to the receiver.

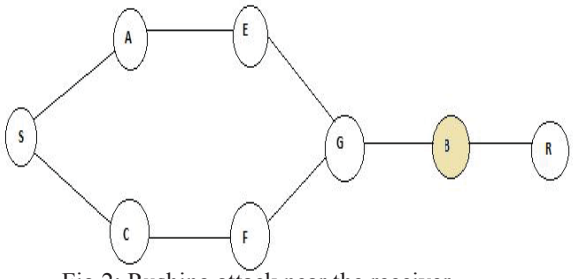

Fig.2: Rushing attack near the receiver.

iii) Infested node is anywhere between the sender and receiver:-

Here F is the infested node, this node can be placed anywhere in between the sender and receiver. Packets are transferred from either A or C, packet will reach the receiver through F because through this infested node packet will reach the receiver quickly.

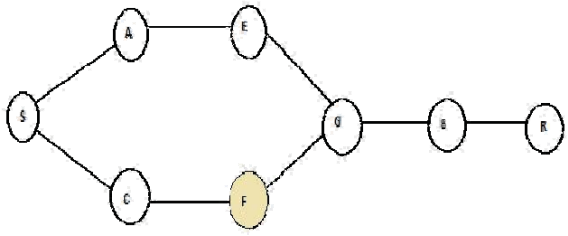

Fig.3: Infested node is in between the sender and receiver.

In present scenario, probability of delivery is more, it is further observed that terminals near are prone to error.

Packet Delivery Ratio (PDR): Total packets received by destination / Total packets dropped by destination [4].

Packet Drop Ratio (PDrR): Average packets dropped / Total dropped [4,6].

Average Delay: It shows average delay between sending and receiving of packet as a consequence of acquisition, buffering, processing and retransmission [5].

III. METHODOLOGY

Data Collection methods:

Data simulation results are extracted from trace files [4].

Simulation Results:

TABLE 1: SIMULATION ENVIRONMENT

Channel type	**Channel/ Wireless Channel**
Radio-propagation model	Propagation/TwoRayGround
Antenna type	Antenna/Omni Antenna
Link layer type	LL
max packet in ifq	50
network interface type	Phy/Wireless Phy
MAC type	Mac/802_11
routing protocol	AODV/DSDV
Topology	1186x584
Finish time	100
Number of nodes	25-30
Mobility	Mobile
Simulator	Matlab

A total of 25 nodes were placed in the network and then simulated using the AODV protocol. The simulation environment is according to the details mentioned in Table 1. The simulation was done with 0, 1, 4, 8, 12, 16 and 20 infested nodes. Table 2 highlights the various observations made under different situations.

TABLE 2:- RESULTS OF DIFFERENT PARAMETERS TESTED

	No of Nodes	**No of nodes infected**	**% of nodes infected**	**No of packets sent**	**No of packets Received**	**Packet delivery ratio**	**Packet drop Ratio**	**Average delay**
Without attack	25	0	0%	85000	83912	99.4 %	0.0064 %	92344.3
With Rushing Attack	25	1	4%	85000	78642	93.11%	7.39 %	92310
	25	4	16%	85000	77044	91.2%	9.6 %	92288.5
	25	8	32%	85000	76772	90.9 %	10 %	92262.8
	25	12	48%	85000	75412	89.2 %	11.99 %	85652.9
	25	16	64%	85000	74800	88.5 %	12.9 %	85322.3
	25	20	80%	85000	71400	84.5 %	18.29 %	85157.7

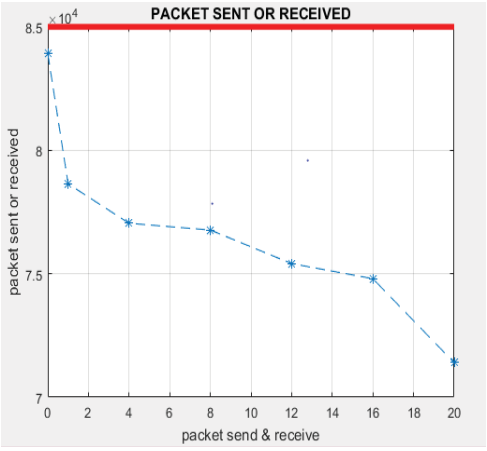

Fig. 4: No of Packets Sent and Received with affected nodes.

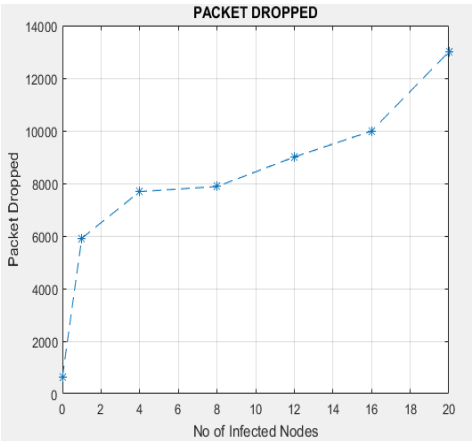

Fig.5: No of packets dropped

It was found that with increase of attacker nodes the Packets received/throughput decreases proportionally.

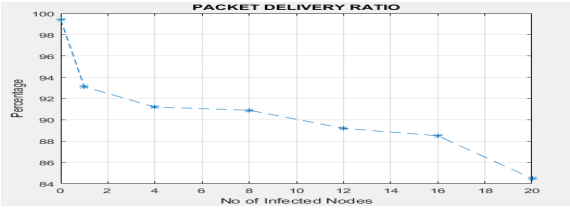

Fig 6: Packet Delivery Ratio

C

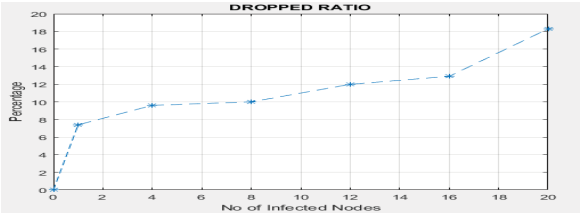

Fig 7: Packet Drop Ratio

Simultaneously Packet Drop Ratio increases with increase of attacker nodes. The more the infected node in the network more will be the Packet Drop Ratio as illustrated in fig 7.

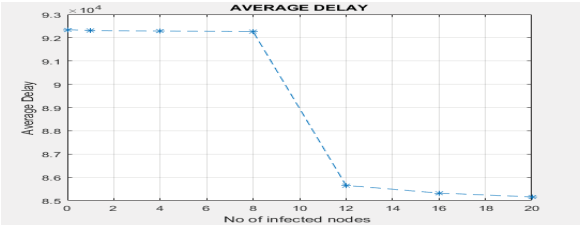

Fig 8: Average Delay

The delay is less as the packet request is sent quickly by the infected nodes and as the no. of infected nodes increases the packets are transmitted faster through those nodes and as a result the average delay decreases as depicted in fig 8.

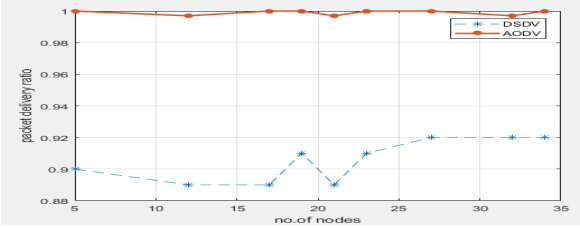

Fig.9: AODV Vs DSDV

The proposed system performance is later evaluated for DSDV routing protocol for 25 to 30 active nodes under similar scenario and it is found that performance of the AODV routing protocol is marginally better than DSDV as presented in fig 9.

IV. CONCLUSION & FUTURE SCOPE

As per experimentations, it is evident that whenever there is no infested node, the reported packets dropped are found to be extremely low and efficiency in terms of packets deliverered is observed as 99%. With the introduction of infested node, number of packets dropped starts to increase and delay starts to decrease. Eventually, when there are maximum numbers of infested nodes in that network, performance worsens with Packet Delivery Ratio going down to about 84%.

Thus it can be concluded that such attack leads to dropping of packets depends on the number of infested nodes. Later performance comparison made between two routing techniques have shown better results for AODV, it can be further tested for other major techniques like DSR & ABR.

V. REFERENCES

[1] Meena Bharti, Manish Goyal, Rajan Goyal, “Detection of rushing attack by comparing energy, throughput and delay with AODV”, International Journal of Computer Science (IIJCS), Volume 2, Issue 11, November 2014.

[2] Seyed-Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin, Hassan Chizari, “Rushing Attack Against Routing Protocols in Mobile Ad-Hoc Networks”, International Symposium on Biometrics and Security T echnologies (ISBAST) , IEEE, 2014.

[3] Shyamala Ramachandran, Valli Shanmugam, “Performance Comparison of Routing Attacks In MANET And WSN”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.3, No.4, August 2012.

[4] Sukiswo, Muhamad Rifqi Rifquddin, “Performance of AOMDV Routing Protocol Under Rushing and FloodingAttacks in MANET ”, 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Indonesia, 2015.

[5] Sandeep Kumar Arora, Himanshu Monga, "Performance evaluation of MANET on the basis of Knowledge Base Algorithm ", International journal of Light & Electron, Optik. Elsevier, Volume 127, Issue 18, September 2016, Pages 7283-7291

[6] Latha T amilselvan, V. Sankaranarayanan, "Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks", International Symposium on Ad Hoc and Ubiquitous Computing, Pp. 42-47, 2006.

[7] Sandeep Kumar Arora , Himanshu Monga, " Combined Approach for the Analysis of Black Hole and Worm Hole Attack in MANET", Indian Journal of Science and Technology, Vol 9(20), DOI: 10.17485/ijst/2016/v9i20/90391, May 2016.

[8] Taruna S., Purohit G.N. (2011) Scenario Based Performance Analysis of AODV and DSDV in Mobile Adhoc Network. In: Meghanathan N., Kaushik B.K., Nagamalai D. (eds) Advances in Networks and Communications. CCSIT 2011. Communications in Computer and Information Science, vol 132. Springer, Berlin, Heidelberg.

[9] M. Becker, S. Schaust, and E. Wittmann, “Performance of routing protocols for real wireless sensor networks,” in Proceedings of the 10th International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS '07), San Diego, Calif, USA, July 2007.

1.