Capability Analysis of Attacks in Wireless Sensor Network

Neha Singh[1], Dr. Deepali Virmani[2]
[1]University School of ICTGGSIPU,New Delhi, India
[2]Department of Information Technology, BPIT, GGSIPU,New Delhi, India

Abstract-Security is key concern area in WSN as the nature of such networks makes them susceptible to various types of attacks. Driven by this, a lot of research work has been done to classify the attacks and their prevention schemes. In this paper, some well-known attacks are compared based on their severity in WSN. The behavior of black hole, gray hole and flooding attack is simulated and analyzed using ns2. The capability analysis is done on the parameters such aspacket delivery ratio, throughput, drop rate, success rate and density of packet drop, packet forward, packet sent and packet received. The analysiscompares the intensity of the attacks against each other. The simulated result shows a maximum density of packet drop in black hole attack and a minimum density of packet received in flooding attack.

*****

1. INTRODUCTION

Since years, research community drew abundant consideration on various issues of wireless sensor networks ranging from theoretical to practical applications [1].

Wireless sensor network is the network of sensor nodes connected to other nodes and arranged in different topology that promises to facilitate real-time data processing [2][3].

These networks comprise of nodes, which are low cost, low power and self-organize sensor nodes and perform their respective functions in the network. The sensor nodes are hundred or thousand in number and highly distributed inside the system [4].

These sensor nodes are used in various fields like in military areas, tracking weather conditions, monitoring underwater water activities etc. [3].

Various types of wireless sensor networks are used in almost every field, for example in terrestrial wireless sensor network, sensor nodes are diffused into target areas in random or pre-planned manner. Similarly, in underground WSNs the sensors are hidden underground like cave or mine for checking the conditions. But with all these WSN there are different issues related with the nodes like signal strength fading, their battery life, their cost etc. [4].

WSN is unshielded from various types of passive and active attacks because of its ad-hoc nature.

Attacks can be categorized in two broad categories: Passive and Active Attacks.

Passive attack is based on the location of attacker, placed outside the network and does not have direct affect on network. Some examples of such attacks are eavesdropping where the knowledge about information can be gained through constant hearing by a mischievous node. Another example is Traffic Analysis where the node with immense activity can be figured out by analyzing the traffic of the network and once the node with high activity is found then mischievous node harms it [5].

Active attacks cause interruption in the communication of network. Some examples of active attacks like Selective Forwarding and Wormhole Attack. In Selective Forwarding attack, mischievous nodes may drop packets and assure the messages are not further propagated in the network [6]. It is the special form of black hole attack and because ofthe unreliable communication these attacks are not easy to identify and degrades the efficiency of network. In Wormhole Attack, mischievous node route the packets through some fake shortcut path. These attacks are easy to inject in the network by attacker and hard to detect[7].

In this paper, the type of attacks in wireless sensor networks is analyzed. The quality parameters are identified in terms of best to worst.

The remainder of this paper is organized as follows: In Section 2, Some background information on sensor network, including analysis of attacks, a capability analysis of attacks in sensor network is introduced. Section 3 gives the capability analysis for the simulation and comparison of parameters in WSNs. In Sections 4, simulated results are presented. Section 5 concludes the paper by emphasizing our contributions and discusses future work.

2. BACKGROUND

One of the DOS attacks is the Blackhole attack, which seems to be occurred when multiple nodes are captured and reconfigured so as to block the receiving packets, which cause long delays as those packets do not reach the destination [8]. Blackhole attack is categorized in two types: External Blackhole, where external node act as intruder and Internal Blackhole, where node inside the network behaves as intruder [14]. In paper [8] various network parameters are used to measure the affect of blackhole attack on the network. The author proposed an algorithm, which is capable of detecting and preventing the network from the attack. In paper [17] the author presented an authenticated end-to-end acknowledgment based approach, which verify the correct forwarding of packets by intermediate nodes in simple or cooperative manner.

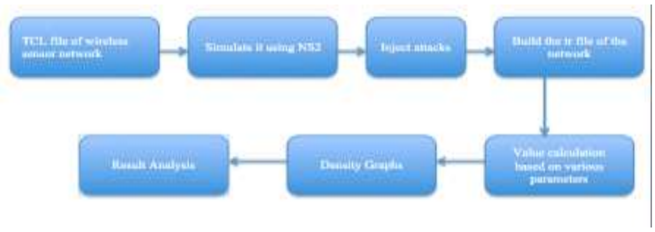
Gray-hole attack is the specific form of Black hole attack where some packets are allowed to pass thorough and some packets are selectively dropped [9]. These attacks are difficult to detect because of random behavior of packet dropping. Here mischievous node initially acts as truthful node to find network route and after that quietly drop packets in probabilistic way [16]. Thus greyhole nodes are detected and are not given priority while selecting route for packet transmission in the network [15].

Whereas in flooding attack the intruder bombards large quantities of junk packets to all the other nodes in the network that results in exhaustion and depletion of the resources and the network bandwidth [10]. In paper [18] the author discussed various existing attack prevention techniques and proposed an improved approach for DOS attack, which will upgrade the precision of attack prevention, decrease the incorrectness of the system.

3. Proposed Capability Analysis Framework of various attacks

Proposed Capability analysis framework presents the framework for the analysis of various attacks. CAF represents various steps followed for capability analysis.

The simulation is done on NS2 simulator. CAF is represented by fig 1:


TCL file of wireless sensor network
Simulate it using NS2
Inject attacks
Build the tr file of the network
Value calculation based on various parameters
Density Graphs
Result Analysis

CAF is applied on three famous attacks and are compared on the parameters packet delivery ration, throughput, success rate, drop rate and density of packet sent, packet receive, packet drop and packet forward.

4. Parameters for Capability Analysis

4.1. Packet delivery ratio-

Packet delivery ratio (Pdr) is the measure of calculating the ratio of number of packets received to the total number of packets actually sent by the sender towards the destination. It is desired that PDR should remain as high as possible. PDR directly shows the reliability of data transmission in the network and the loss rate. The measure is very important, especially for energy constrained networks as it directly affects the lifetime of the network [11]. Packet delivery ratio depends on various factors such as network density and traffic load [12] but keeping them constant, we need to find out the PDR under various types of attacks.

$$Pdr = \sum_{1-n}^{t} \left(\frac{S_p}{R_p}\right) * 100$$

wherePdr is Packet delivery ratio,
$S_p$is Send Packets,
and$R_p$is Receive packets

4.2. Throughput

Throughput is the ratio of number of packets received by the destination (in terms of bits) to the time elapsed between the first and last received packets. Throughput and PDR described above goes hand in hand. Predicting throughput is a challenging task in networks with different source data routes [13]. It describes the average rate of successful data delivered across the WSNs. The importance of throughput varies according to various applications, like for medical and industrial applications throughput is very important but when sensor nodes are deployed in hostile environments the network lifetime is more important.

$$Throughput = \sum_{1-n}^{t} \left(\frac{R_p}{T_t}\right) * 100$$

whereT_t is Transmission Time
and$R_p$is Receive packets

4.3. Drop Rate

Drop Rate is defined as the rate at which packet dropping takes place. It affects WSN in various ways as it increases the bandwidth wastage and the delay in transmission of packets. Mathematically, it can be defined as

$$Drop\ Rate = \sum_{1-n}^{t} \left(\frac{S_p - R_p}{S_p}\right) * 100$$

$S_p$is Send Packets,
and$R_p$is Receive packets

4.4. Success Rate

Success Rate is defined as the rate at which the packets are successfully transmitted from the source to destination in the assigned time i.e. without any delay.

$$Success\ Rate = \sum_{1-n}^{t} \left(\frac{R_p}{S_p}\right) * 100$$

$S_p$is Send Packets,
and$R_p$is Receive packets

4.5. Density

The density is calculated as the number of packets per unit time.

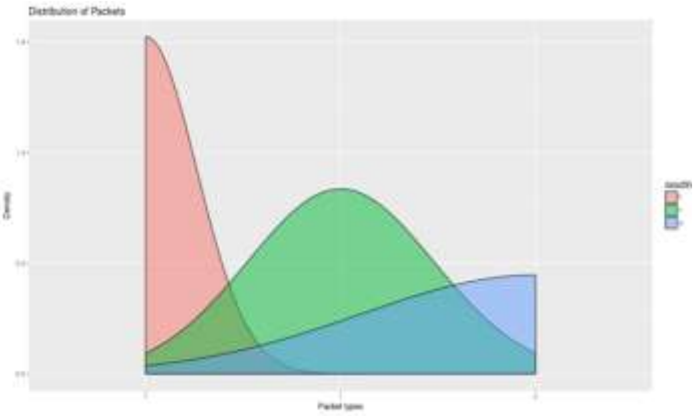


Figure 2 shows the density plot for no attack. Simulation results clearly show that when there is no attack in the network, there is no packet drop. The maximum density of the parameters packet forward, packet received and packet sent is 1.55, 0.80, and 0.45 respectively.

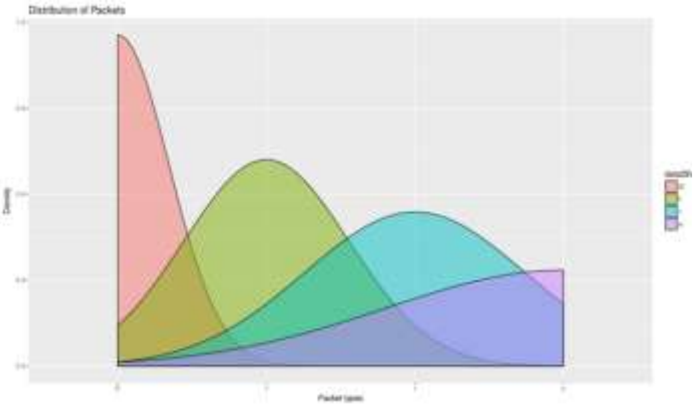


Figure 3 shows the density plot for black-hole attack. Result shows the significant amount of density of packet. The density of packet drop reaches a maximum of 1.125 and then it gradually decreases.

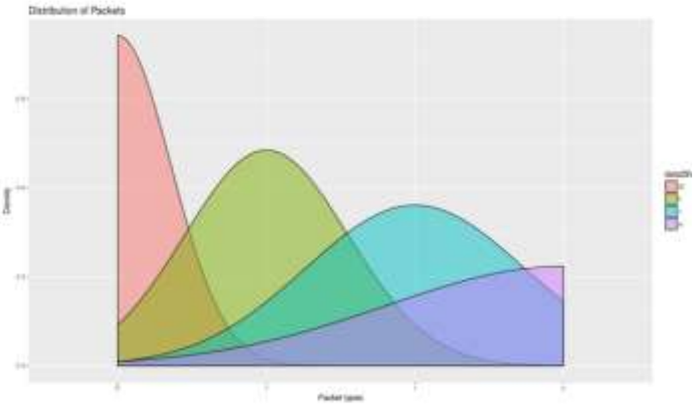


Figure 4 presents the density plot for grey-hole attack. Result proves large amount of packets to be dropped. The maximum density of packet drop is seen as 1.1.

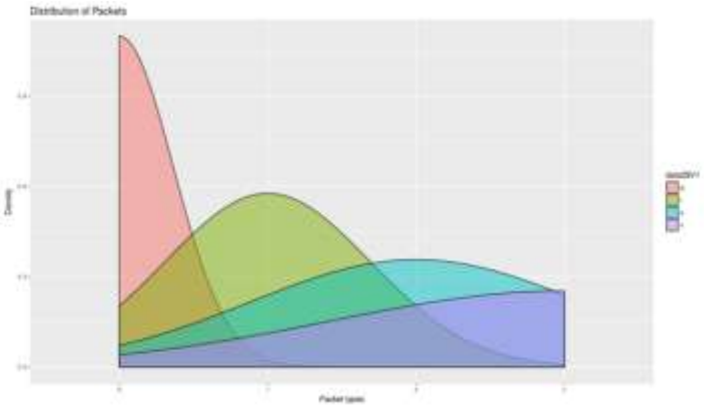


Figure 5 presents density plot for flooding attack. Introduction of flooding attack in a wireless sensor network induces packet drop. The maximum density of packet drop is observed to be 1.1.

Final results of density drop are given in the table:

Attack\density of Parameters	No attack	Black-hole attack	Grey-hole attack	Flooding attack
Packet sent	0.45	0.33	0.33	0.33
Packet Receive	0.8	0.54	0.55	0.58
Packet Drop	0	1.125	1.1	1.1
Packet Forward	1.55	0.7	0.69	0

5. Simulation Result Analysis

NS2 simulator is used for Capability analysis. Simulation Parameters used are shown in the table2.

Table 1: NS2 Simulator Parameters

MAC layer protocol	IEEE 802.11
Data Rate	1 packet/second
Routing Protocol	AODV
Number of mobile nodes	16
Effective Simulation time	100 sec
Grid Size	4*4

For simulation grid deployment is used with 4x4 grid. 16 sensor nodes are placed on the grid. Mischievous node is placed in between the sender and receiver node. Sensor nodes send data at 1 packet/second.

The comparative analysis for the three attacks is based on the parameters packet delivery ratio, throughput, success rate, drop rate and density of packet drop, packet forward, packet sent, packet received. The comparison is shown in the following figures.

Black hole attack have a zero throughput and zero success rate whereas grey hole and flooding attack have 190, 15.96

and 140,11.76 throughput and success rate respectively. The packet delivery ratio goes to infinity for black hole attack and remains 626.315 and 113.33 for grey hole and folding attack respectively.

The success rate is minimum for black hole attack continued with flooding and least minimum for grey hole attack. The most intense attack out of these three attacks is the flooding attack.

Fig 6 shows the packet forward and packet drop in a no attack situation and in various attacks situation. Number of packets forwarded in no attack WSN is 489, whereas in grey-hole attack, 77.7% packets were forwarded, in black hole 74% of packets were forwarded and in flooding attack zero packets were forwarded. Similarly, packet drop is zero in no attack WSN and it increases to 31% in grey-hole attack, 32% in flooding attack and 37% in black-hole attack.

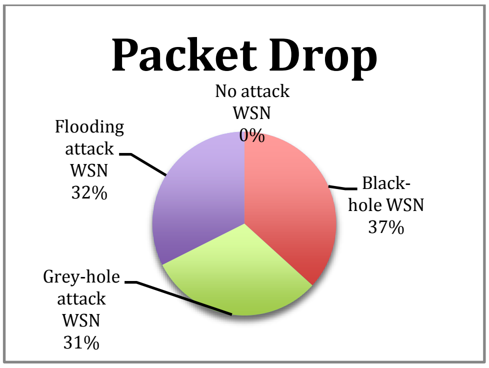


Fig. 6 Packet Drop

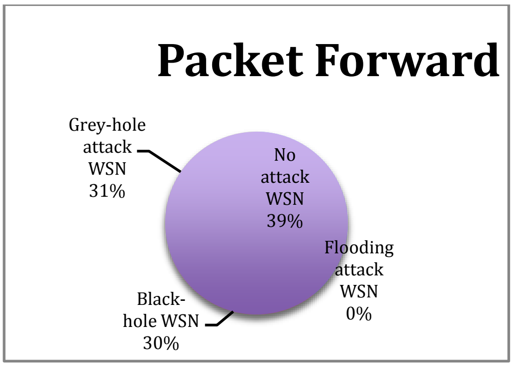
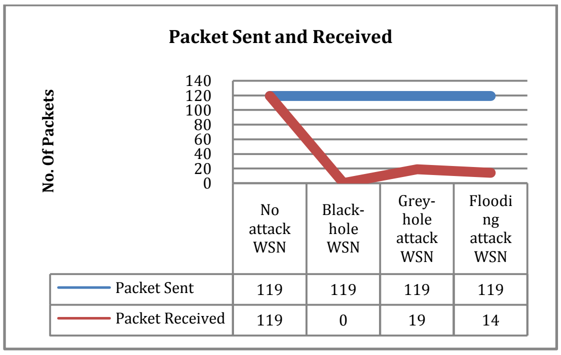


Fig. 7 Packet Forward

The comparison results of packets sent and received are shown in figure 8.

Fig 9 shows the analysis of above discussed quality parameters in WSN.



	No attack WSN	Black-hole WSN	Grey-hole attack WSN	Flooding attack WSN
Packet Sent	119	119	119	119
Packet Received	119	0	19	14

Fig. 8 Packet Sent and Received

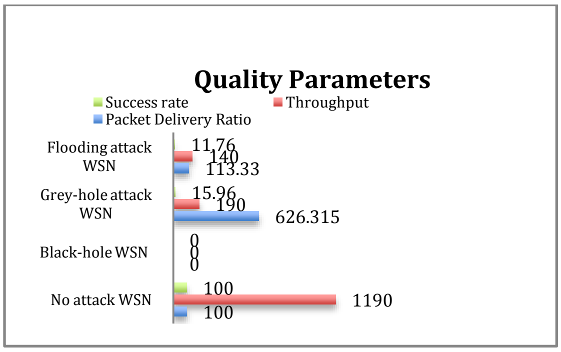


Fig. 9 Quality Parameters

6. CONCLUSION

In this paper various attacks in WSN are studied and compared. The simulation of various attacks in WSN is performed and observed. A density plot against each attack is plotted and compared with a no attack situation. When the density was zero, the flow was observed to be zero against send, received and dropped packets. When the flow of the packets gradually increases, the density against each parameter also starts increasing. When more and more packets get added to flow, it reaches a saturation point and gradually a drop in density is observed thereafter in each case. The scenario is changed from malicious to non-malicious mode in each attack case and performance is evaluated based on the quality parameters. In case of no attack, the density of the send packet, received packet and packet forward is observed to be maximum at 0.45,0.66 and 1.55 respectively. There is no packet drop in a no-attack situation but when various attacks are introduced the maximum density of packet drop is observed to be 1.125, 1.1 and 1.1 for black hole, grey-hole and flooding attack respectively.Simulation results proved that there was 31% packets drop in grey-hole attack, 32% packets drop in flooding attack and 37% packets drop in black-hole attack. The success rate is minimum for black hole attack continued with flooding and least minimum for grey-hole attack. The most intense attack out of these three attacks is the black-hole attack. In our future work, we will find a prevention technique for flooding attack.

REFERENCES

[1] Li, N., Zhang, N., Das, S. K., &Thuraisingham, B. (2009). Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Networks*, *7*(8), 1501-1514.

[2] Zhang, F. J., Zhai, L. D., Yang, J. C., & Cui, X. (2014). Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. *Procedia Computer Science*, *31*, 711-720.

[3] Patil, A., &Gaikwad, R. (2015). Comparative Analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Network. *Procedia Computer Science*, *48*, 387-393.

[4] Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., &Qureshi, K. N. (2014). Security issues and attacks in wireless sensor network. *World Applied Sciences Journal*, *30*(10), 1224-1227.

[5] Virmani, D., Soni, A., Chandel, S., &Hemrajani, M. (2014). Routing attacks in wireless sensor networks: A survey. *arXiv preprint arXiv:1407.3987*.

[6] Bysani, L. K., &Turuk, A. K. (2011, February). A survey on selective forwarding attack in wireless sensor networks. In *Devices and Communications (ICDeCom), 2011 International Conference on* (pp. 1-5). IEEE.

[7] 7.Nagrath, P., & Gupta, B. (2011, April). Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* (Vol. 6, pp. 245-250). IEEE.

[8] Wazid, M., Katal, A., Sachan, R. S., Goudar, R. H., & Singh, D. P. (2013, April).Detection and prevention mechanism for blackhole attack in wireless sensor network. In *Communications and Signal Processing (ICCSP), 2013 International Conference on* (pp. 576-581). IEEE.

[9] Schweitzer, N., Stulman, A., Shabtai, A., &Margalit, R. D. (2016). Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks. *IEEE Transactions on Mobile Computing*.

[10] Dharini, N., Balakrishnan, R., &Renold, A. P. (2015, May). Distributed detection of flooding and gray hole attacks in Wireless Sensor Network. In *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on* (pp. 178-184). IEEE.

[11] Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. *Ad Hoc Networks*, *6*(1), 32-46.

[12] Indra, A., &Murali, R. (2014). Routing protocols for vehicular adhoc networks (VANETS): a review.

[13] Murdiyat, P., Chung, K. S., & Chan, K. S. (2014, October). Predicting the network throughput of wide area WSN in rural areas. In *Communications (APCC), 2014 Asia-Pacific Conference on* (pp. 106-111). IEEE.

[14] Kaur, R., & Singh, P. (2014). Review of black hole and grey hole attack. *The International Journal of Multimedia & Its Applications*, *6*(6), 35.

[15] Bhalaji, N., &Shanmugam, A. (2012). Dynamic trust based method to mitigate greyhole attack in mobile adhoc networks. *Procedia Engineering*, *30*, 881-888.

[16] Banerjee, S. (2008, October). Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In *proceedings of the world congress on engineering and computer science* (Vol. 2008).

[17] Baadache, A., &Belmehdi, A. (2014). Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. *Computer Networks*, *73*, 173-184.

[18] Patil, S., &Chaudhari, S. (2016).DoS Attack Prevention Technique in Wireless Sensor Networks. *Procedia Computer Science*, *79*, 715-721.