Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks

Abdullah Aljumah, Tariq Ahamed Ahanger

College of Computer Engineering & Sciences
Prince Sattam Bin Abdulaziz University, KSA

Abstract

Wireless sensor networks are vulnerable to many devastating threats and blackhole (DoS-DDoS) is a very common threat for not being easy to detect and defend, thus declining the performance of the network and the system. The attackers select a set of client nodes in the network and reconfigure them to drop the received packets instead of forwarding them to the nest node or towards the destination node , resulting in a situation where packets enter the blackhole area but never reaches the destination resulting in higher end-to-end delay and decline in the throughput. A good amount of research has been done during the recent past for detection and prevention of this type of attack so as to maintain the performance and reliability of the wireless sensor networks. In this research article, the impact of blackhole traffic is evaluated using network basic parameters and a novel technique is designed to detect and prevent the blackhole attack in wireless sensor networks.

Keywords:
WSN, DoS, DDoS, Blackhole, Security.

1. Introduction

Wireless sensor networks aka WSN also known as wireless sensor and actuator networks (WSAN) are collection of sensors nodes grouped together for collection of wide range of mission critical data such as acoustic signals, pressure, temperature, application [1]. This special feature has made them of special importance for vigilance in military installations, health care monitoring, industrial data gathering, traffic monitoring, signaling systems of railways, coal mines etc [2]. Wireless sensor networks are composed of tiny, cheap devices known as nodes interfaced with some sensors to sense changes in ambient physical environment. Data gathered by these nodes are periodically uploaded or updated to a distant high end node also known as Base Station (BS) or Sink [3]. These tiny nodes are often powered by small dry cell batteries but some sophisticated implementation may have support of non conventional energy sources like solar power etc. unlike peer to peer communication of legacy networks these nodes are designed and configured to sense and disseminate these sensed data.

Since data collected by wireless sensor networks is precious and raw, its security is a prime concern. Implementation constraints like deployment conditions of nodes, wireless communication media, limited power backup etc. make situation more vulnerable [4]. These small devices (nodes) have more susceptibility for attacks than normal wireless networks and even more than to wired networks. Approximately all kinds of attack mechanism existing in wired and wireless networks have been introduced gradually in wireless sensor networks as well. Classical techniques to prevent and to mitigate such attacks are not suitable for wireless sensor networks because of limited capabilities of wireless sensor nodes [5]. Number of attacks on wireless sensor networks are increasing rapidly. Day by day these attacks are growing in number as well as in complexities of attack launch. Attacks are causing increasingly bigger losses and damages to industries and businesses [6]. Attack types and their modus operandi have been studied in length in recent past. WSN suffers both internal as well as external attacks. While black hole, grey hole, sink hole etc. are internal attacks DoS, sniffing, eavesdropping etc. are few widely used external attacks types [7]. An attack can be passive if it only captures the packet, copies it and then forwards to seek destination node without altering it. Most of the preventive measures in wireless sensor networks for passive attacks rely on cryptographic solutions to make data secure even if captured/sniffed by external agents, whereas an Active attack captures the data alters it and then forwards to intended node or sometimes hinders the availability of required nodes and requires dedicated efforts to be made to mitigate attack.

2. Black Hole Attack:

A black hole attack is an external attack where an external adversary (not part of network) attacks wireless sensor network or precisely part of network. This adversary by applying several techniques lures nodes sending packets to Base Station as having shortest path available, consequently when nodes start sending data packets through this illusive path, it simply drops the packets [18]. Resulting in, in consistency of data received at Base Station.

lackhole is a denial of service (DoS) attack in which a router relays or drops data packets instead of discarding

Manuscript received February 5, 2017
Manuscript revised February 20, 2017

for a specific network destination at specific time – a packet after every n number of packets or after every t number of seconds. It is slightly different from black hole as black hole is a general denial of service (DoS) attack that drops packets as its key constraints are very specific. It is an active attack that leads dropping of packets. The attacking node at first agrees to forward data packet or messages then fails to do so and starts behaving like a malicious node. At first the attacker node behaves normally and replies true route replies(RREP) messages to other nodes to invoke route request (RREQ) messages and accepts or takes the sending packets and finally drops few or all packets to launch denial of service (DoS) attack. If nodes in the neighborhood try to send data packets over attacking or victim nodes lose connection to target or destination node or network and may want to discover or rebuild a route again by broadcasting route request (RREQ) messages. Attacking node send route reply (RREP) messages to establish route. This process doesn't stop until attacking node achieves its goal like battery power consumption, bandwidth consumption etc.

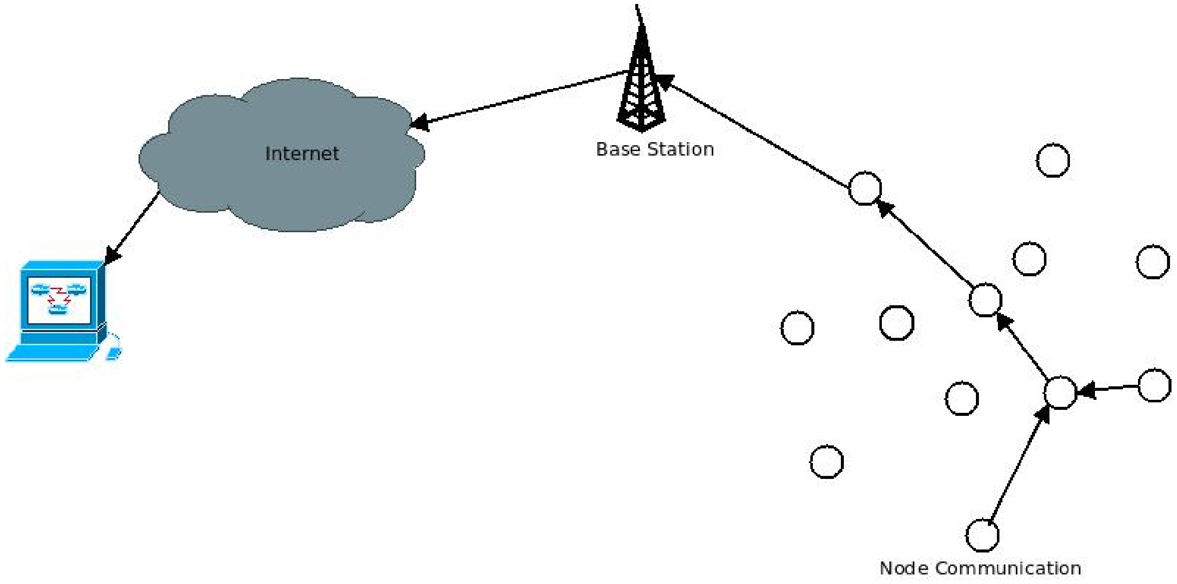

Fig. 1(a) - Normal node communication in a Typical WSN

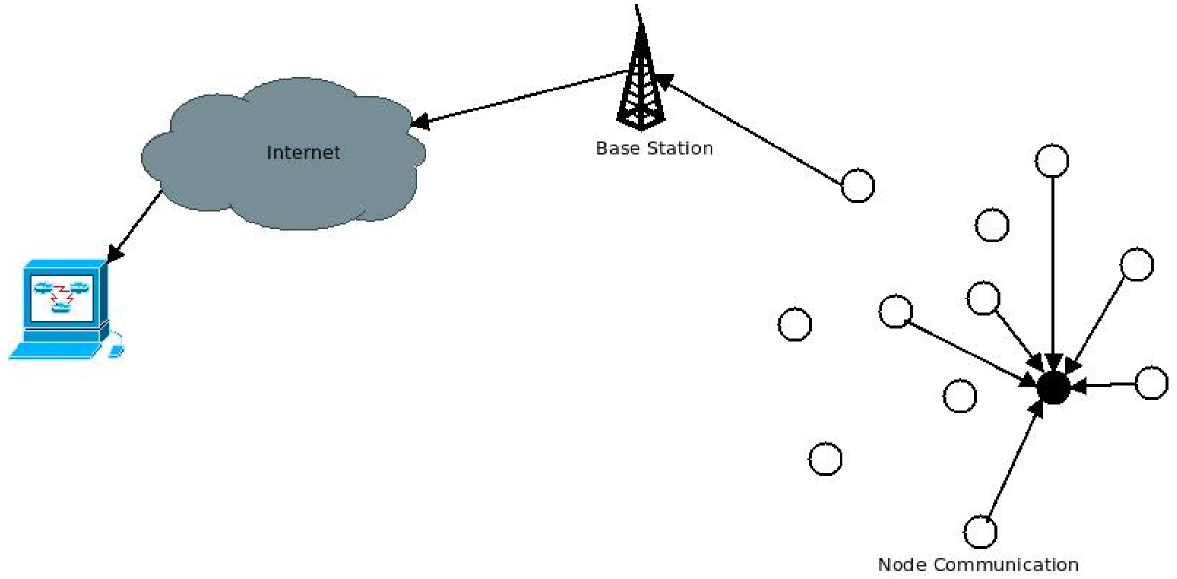

Fig. 1(b) - Node communication in a Compromised WSN

3. Related Work

B.Yu proposed use of checkpoints for detection of Grey holes in wireless sensor networks. These checkpoints are randomly chosen among the network nodes. These nodes when receive data packets generate acknowledgement packets which are passed to upper level nodes. During transmission of data packets if any checkpoint doesn't receive enough acknowledgements, it produces warning packets which are disseminated in the network in order to raise awareness about presence of black hole/ grey hole [8].

Jiang proposed a method relying on mutual trust level among nodes and packet loss to detect selective forwarding attacks. When network connections are setup for a given topology and communication starts for a certain path, intermediate nodes keep record of number of packets received and number of packets forwarded; these statistical details are uploaded to BS periodically. BS computes mutual trust level of nodes from this statistical data and assesses packet lost during communication path to determine if there is a Black hole or grey hole[9].

Yu and Xiao, discussed mechanism of raising alarms based upon multi-hop acknowledgement received from intermediate nodes of a communication path. Every node in a communication link has responsibility of detecting malicious nodes around it, if any suspicious activity is detected by any of the intermediate node in the upward/downward communication path, it raises alarm packets for source node/ base station using multi-hops [10].

Sophia Kaplantzis et al came up with a novel idea of centralized intrusion detection which uses Support Vector Machines (SVM) and sliding window for prediction of presence of Black hole/ Grey holes in the network. Being a centralized intrusion detection scheme all necessary computation for intrusion detection takes place in Base Station and hence sensor nodes are no way required to contribute in this activity preserving their already scarce energy. A high level of accuracy could be obtained without depleting motes energy by the scheme [11].

Brown and Xiaojiang have proposed a mechanism of hierarchical structure of nodes viz. Heterogeneous Sensor Network (HSN). A HSN is made of two types of nodes, Powerful High end sensors or H sensors and Large number of Low end sensors or L sensors, once deployed cluster s are formed with H sensors as cluster heads [12].

Xin, etal. Proposes a collaborative low cost scheme for detection of black holes where every neighbor takes part in detection of black holes in its surrounding. These neighbor nodes monitor a commuincation and keep check on packet dropping, if any packet is dropped they simply resend it; these monitoring nodes are configured in a WSN mesh topology [13].

Zurina Mohd Hanapi et al proposed a scheme especially suited for CTS rushing and consequently black hole and grey holes. Their approach is based on Dynamic Window Stateless Routing Protocol. Without altering very basic structure of Dynamic window stateless routing protocol, the dynamic window stateless implicit geographic forwarding DWSIGF delivers a promising defense for Black holes and selective forwarding attacks [14].

Riaz Ahmed Shaikh et al proposed a novel idea of using two new variables viz. Route and location privacy and data sensed privacy algorithms for wireless sensor networks as these feature are intrinsic and inbuilt for wireless sensor networks constraints imposed on motes, deployment condition and motes capabilities. For moderate cost of extra memory and slight energy proposed scheme delivers additional trustworthiness among nodes, experimentally they have shown their scheme provides additional security against various privacy attacks e.g. eavesdropping and hop by hop trace back attacks [15].

Guorui Li et.al has proposed a cost and effort saving scheme viz. sequential mesh test. When packet drop alarm is received, cluster head nodes conducts sequential mesh test for packet dropping. The proposed scheme requires a deficit amount of samples to run test rather than running test for all data samples or on all communication streams, further during the test based upon intermediate results, scheme decides whether to continue test further or stop. Hence it is resource efficient scheme which requires even lesser time for detection of black holes [16].

Deng-yin ZHANG et.al proposed a scheme based on Digital watermarking technology for detection of Black holes / Grey holes. It simply inserts watermarks in the packets being transmitted, when received at Base Station, BS decides if there were packet lost in between communication or has been tampered from the information extracted from watermarks. Simulation results shown efficiency of this scheme [17].

4. Proposed System

Majority of the delay in packet delivery in the network and decline in the throughput is due DoS and DDoS attacks and the most common one is black hole attack and in totality decline the performance of the network.

We have proposed a method of detection and prevention against blackhole attack that detects attacker node and prevents it before it affects the network. In the experimental environment we created clusters using sensor nodes and these clusters contain those nodes which are accessible zone of each other for communication purpose. These sensor nodes elect a cluster coordinator and to be considered as cluster coordinator, it must have the following characteristics.

- Equitability: Any sensor node can be a cluster coordinator which means there is equal possibility for every node to be a cluster coordinator.
- Coherence: A mechanism that choses a sensor node with higher efficiency than others periodically to be the cluster coordinator.

Cluster coordinator is responsible for detecting the intruder node in the cluster once it is selected as cluster coordinator because the cluster coordinator supervises all the sensor nodes in the cluster. This is done with the help of a table maintained by the cluster coordinator containing ID's of all the immediate and intermediate sensor nodes as shown in table 1.

Table 1: ID Assignment

Node	Assigned ID
Router 1 – R1	ID_R1
Router 2 – R2	ID_R2
Router 3 – R3	ID_R3
..	..
..	..
Router n –Rn	ID_Rn

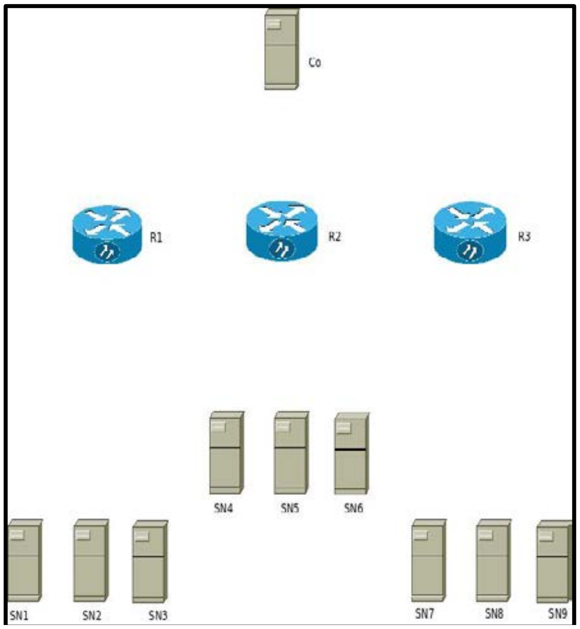

Fig 3: Cluster Formation

Cluster formation and the process of assigning ID to sensor nodes in the current network is shown in figure 3X. Cluster coordinator is denoted Co and the immediate routers R1,R2& R3 report to the Co. while as the sensor nodes are represented by SN1,SN2,…SN9 which sense the physical occurrences and events , convert them into meaningful information and send to the routers.

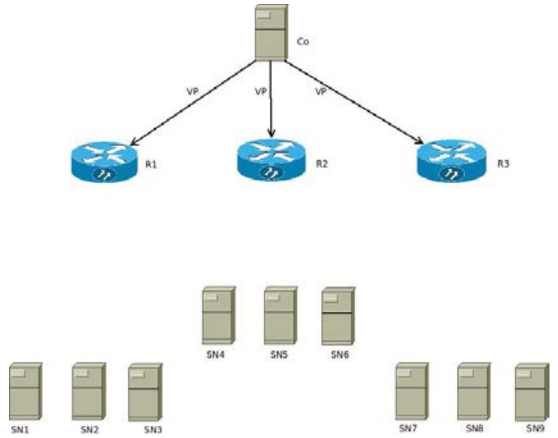

Fig 4: Co Sending VP to routers

The cluster coordinator sender validation packet (VP) to every sensor node in the network that contains the ID of the immediate node as shown in figure 4 and an extra bit to help in recognizing that this is a validation packet. This process is called validation process (stage 1) and the structure of validation packet is shown in figure 5.

ID_R1	Validation

Figure 5: Validation Packet

All the nodes respond with response packet after receiving the validation packet from the cluster coordinator as shown in figure 6.

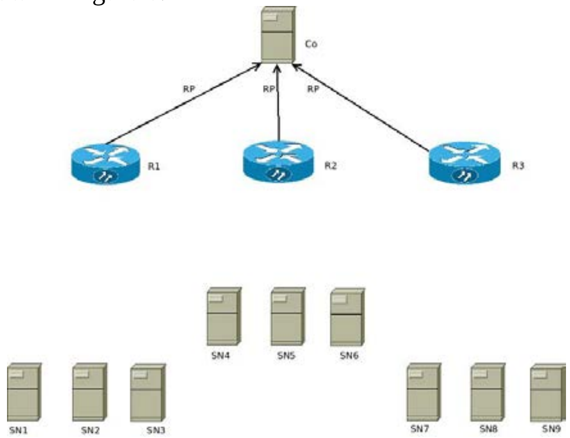

Figure 6: Response packets to Cluster Coordinator

The idea used here is almost same as that of RREQ and RREP as the response packet contains immediate nodes ID and acknowledgement field that certifies and validates that the packet came from a genuine node as shown in figure 7.

ID_R1	Acknowledgement

Figure 7: Response Packet

Normal flow of data in wireless sensor networks is shown in figure 8 where sensor nodes (SN1,SN2..SN9) sense the physical occurrences and events, converts them into meaningful information and forward to the router nodes as sensed data packet. These sensed data packets are further processed by the router nodes and later send to the cluster coordinator as data packet.

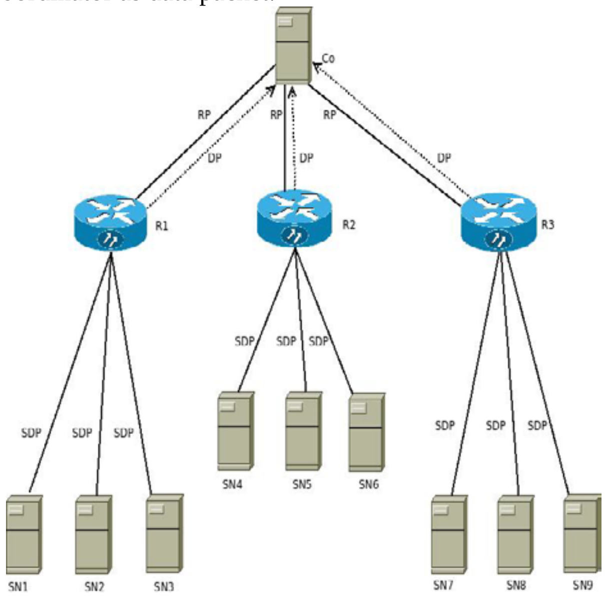

Figure 8: Normal Flow on WSN

In case the cluster coordinator does not receive the response and data packet from the router (e.g Router 1) up to a specified wait time (w_tm), it implies that (Router1) has failed as illustrated in figure 9

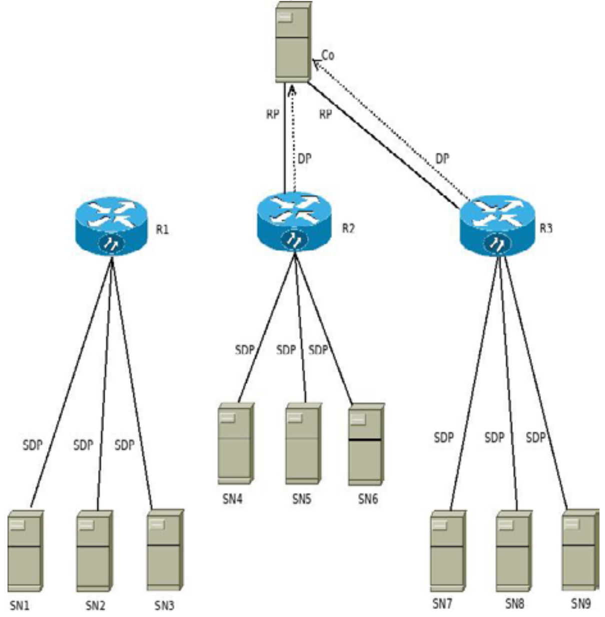

Fig 9: Failed Router

The sensor node send the sensed data packets to the cluster node but router 1 consumes them all and acts like a blackhole instead of forwarding them to the destination as shown in figure 10.

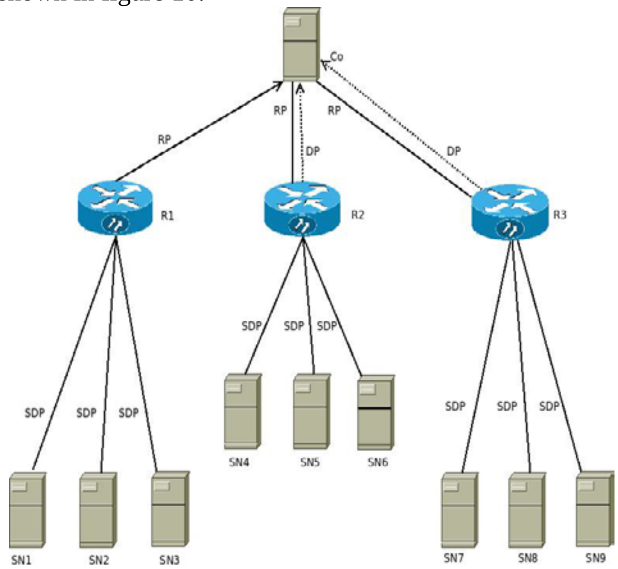

Fig 10: Router 1 acting like blackhole

The cluster coordinator detects the blackhole by its ID as shown in figure 11 because this router (Router 1) is sending response packet but not data packets.

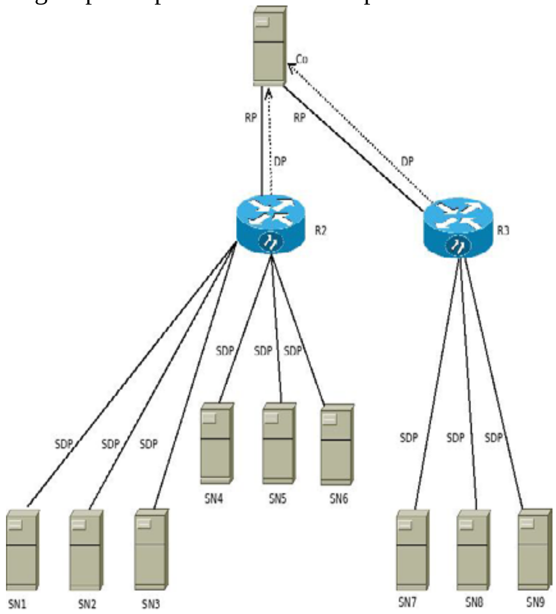

Fig 11: Diverting from R1 to R2

Once the blackhole is detected, the router (router 1) is removed and a cluster is reconstructed. The sensor nodes that were immediate nodes of blackhole (Router1) will now send their sensed data packets to other router

(Router2) in this case. Thus the normal flow in the network is achieved.

Algorithm

```
1.  C  <= { S1, S2, S3, ...., Sn}    //  'C' is a cluster of
    nodes
2.  ID <= { ID1, ID2, ID3, ..., IDn }     //  'ID' is  List
    of node IDs
3.  Si  <= C { Sk} ; k<n                 //  ' Si ' is  a
    selected coordinator
4.  Si <= ID                           // coordinator table
    of node IDs
5.  if res = 'T' and data = 'T'     //  'T' is true
       No Intrusion;
    break to 6;
    else if res = 'F' and data = 'F'     //  'F' is false
    node failure;
    break to 6;
    else if res = 'T' and data = 'F'
            ID <= IDj
            C <=  { S1, S2, S3, ...., Sj-1, Sj+1, ...., Sn  }
    break to 6;
    else
    increment  w_tm        //data packet waiting time
6.  goto 1;
```

5. Evaluation

We used two scenarios for simulation purpose and used the following data as shown in table2 for both the scenarios.

Total Nodes	30	
Total Routers	10	
SN1	R1	Co
SN2		
SN3		
SN4	R2	
SN5		
SN6		
SN7	R3	
SN8		
SN9		
SN10	R4	
SN11		
SN12		
SN13	R5	
SN14		
SN15		
SN16	R6	
SN17		
SN18		
SN19	R7	
SN20		
SN21		
SN22	R8	
SN23		
SN24		
SN25	R9	
SN26		
SN27		
SN28	R10	
SN29		
SN30		

Scanario1: Normal Flow of packets

Sensor nodes SN1, SN2, SN3 report to router 1 and this continue till SN28, SN29 and SN30 report to router 10. And all the routers i.e from router R1 ,R2..R10 report to cluster coordinator Co as shown in Figure 12 in detail.

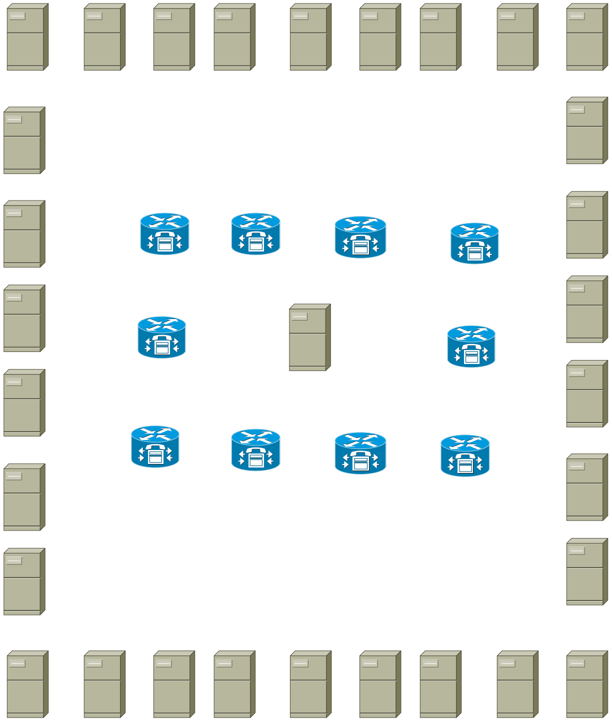

Fig 12: Normal flow in WSN

Scenario 2: Flow of data in Black hole attack

Sensor nodes SN1, SN2, SN3 report to router 1 and this continue till SN28, SN29 and SN30 report to router 10. And all the routers i.e from router R1 ,R2..R10 report to cluster coordinator Co but after the router R1 becomes the black hole , it consumes all the traffic coming towards it from its associated nodes as shown in Figure 13 in detail.

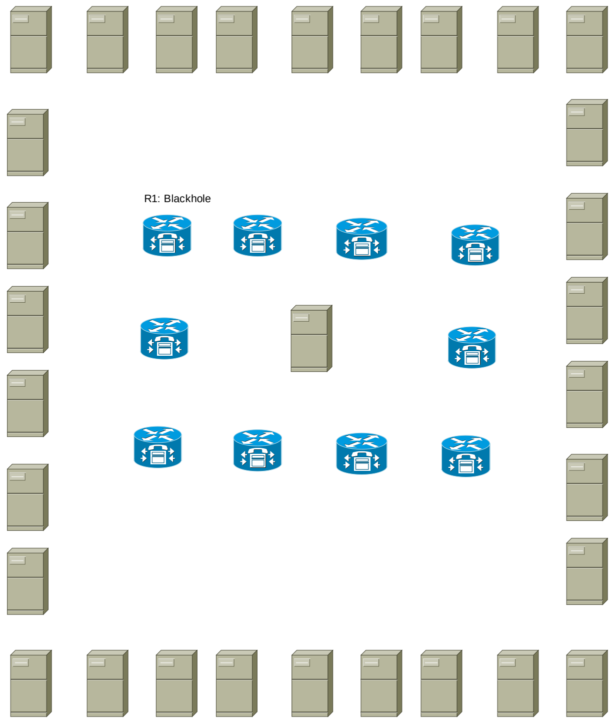

Fig 13: Blackhole (R1) Detected

In normal scenario all the sensor nodes sends their packets towards all the routers which forward them to the cluster coordinator. When router 1, consumes all the packets and becomes blackhole and doesnot forward data to the cluster coordinator. For simulation of this idea we used throughput and end-to-end delay as key fields for statistics

Table 3: Simulation Parameters

Parameter	Value
Simulation Time	59 Seconds
Network Area	1050x525 meters
Network Size	30 Nodes
Normal Scenario	10 Routers
Attack Scenario	1 blackhole and 9 normal
Packet size	1024
Packet arrival time	1
CSMA/CA	Default
Sensing Duration	0.1
Physical Layer	Default

6. Results

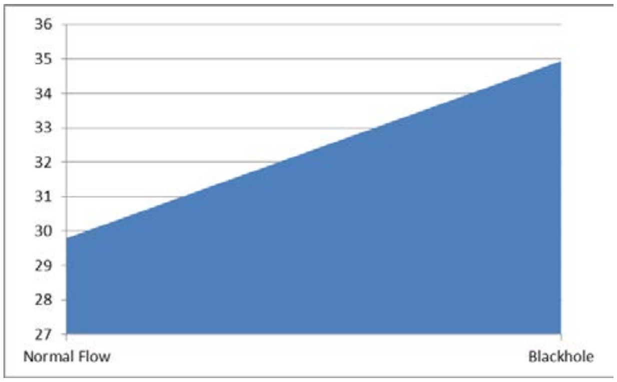

Fig 14: Increase in End-To-End Delay

The comparison of the normal traffic and blackhole attack using end-to-end delay is shown in figure 14 and the figure 15 shows the comparison using throughput

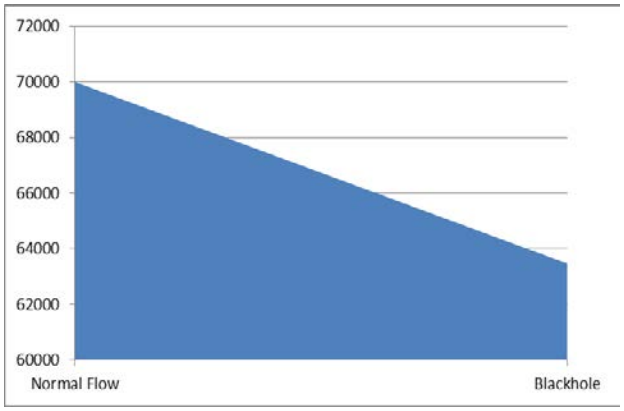

Fig 15: Decline in the throughput

The results clearly showed that end-to-end delay increased from 29.8 to 34.94 and throughput declined from69999.9 to 63467.14.

Conclusion

A detection and prevention method is proposed in this research article. During the experimental evaluation end-to-end delay and throughput, both the parameters were immensely affected when we launched the blackhole attack. The network performance declined so fast due to this attack and the study showed increase in delay time was 5.14 msec and decline in throughput was 6532.76bps. So, there was a great need of designing a powerful method to detect and defend wireless sensor networks from blackhole attacks. In future work, the number of attackers can be increased to check the stability of the method.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2016/2017 under research number 2016/01/6536.

References

[1] M. Al Ameen, J. Liu, and K. Kwak, “Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications,” J. Med. Syst., vol. 36, no. 1, pp. 93–101, 2012.

[2] R. Beghdad and A. Lamraoui, “ Boundary and holes recognition in wireless sensor networks,” J. Innov. Digit. Ecosyst., vol. XX, no. YY, p. ZZ, 2016.

[3] V. Gupta and R. Pandey, “An improved energy aware distributed unequal clustering protocol for heterogeneous wireless sensor networks,” Eng. Sci. Technol. an Int. J., vol. 19, no. 2, pp. 1050–1058, 2016.

[4] D. K. Chaitanya and G. Arindam, “Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation,” Kaspersky.Com.

[5] K. CHELLI, “Security Issues in Wireless Sensor Networks,” Proc. World Congr. Eng., vol. 1, 2015.

[6] M. Islam and S. AshiqurRahman, “Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches,” Int. J. Adv. Sci. Technol., vol. 36, pp. 1–8, 2011.

[7] Z. I. Khan and M. M. Afzal, “Security in Wireless Sensor Networks : DoS Perspective,” International Journal of Engineering Research & Technology (IJERT) vol. 6, no. 1, pp. 311–316, 2017, ISSN: 2278-0181.

[8] B Yu, B Xiao. “Detecting selective forwarding attacks in wireless sensor networks”. In: Proe. of the 20th International Parallel and Distributed Processing Symposium, RhodesIsland, Greeee, 2006,1218 -1230

[9] Jiang changyong, Zhang jianming. “The selective forwarding attacks detection in WSNs”. Computer Engineering, 2009, 35(21):140-143

[10] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th Internation al, page 8 pp., 2006.

[11] Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S ̧ekercio glu ,” Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines”, intelligent sensors, sensor networks and inform ation ,3rd international conference ,pg 335 –340,ISSNIP 2007

[12] Jeremy Brown and Xiaojiang Du. Detection of selective forwarding attacks in heterogeneous sensor networks. In ICC, pages 1583–1587, 2008

[13] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. Pages 226–232, oct. 2009

[14] Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari, Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network”, American Journal of Engineering and Applied Sciences 2 (2): 494-500, 2009.

[15] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d’Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song,” Achieving Network Level Privacy in Wireless Sensor Networks “,Sensors 2010, 10, 1447-1472; doi:10.3390/s100301447

[16] G. Li, X. Liu and C. Wang, "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks," 2010 International Conference on Networking, Sensing and Control (ICNSC), Chicago, IL, 2010, pp. 554-558.doi: 10.1109/ICNSC.2010.5461599

[17] Deng-yin ZHANGa, Chao Xub, Lin Siyuan “Detecting Selective Forwarding attacks in WSNsAuthors

[18] Tariq Ahamad, “Detection and Defense Against Packet Drop Attack in MANET” International Journal of Advanced Computer Science and Applications(IJACSA), 7(2), June 2016