IJIRMET ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 4, April 2017

Selective Forwarding Attack In Wsn

[1] K. Murugan, [2]R.Pravinkumar , [3]A. Joseph Anselm
[1]Research Scholar, [2]PG Scholar, [3]UG Student
Department of Computer Technology
Anna university-MIT Campus, India
[1]krishna.muruga@gmail.com, [2]meetpravinkumar@gmail.com, [3]joeans10313a@gmail.com

Abstract: ***Wireless Sensor Network (WSN) is incorporated in various areas like military, traffic surveillance, healthcare, and monitoring the environmental conditions. Limited battery and low memory are some inherent features which builds impracticable sensor network and it will reduce the communication inefficient. Data attacks related to the sensor nodes which affects the WSNs are wormhole, packet drop and selective forwarding attack. In a packet drop (black hole) attack, one node acts as malicious and also it drops the packets which are forwarded through it. A uniquecharacteristicof this attack is in which the mischievous node drops packets selectively. Network layer is the middle layer that coordinates the lower and upper layers whichplays a vital role for providing the security of WSNs to prevent exploitation of their all kinds of security services. It is importantto analyze and mitigate the security loopholes ofWSNs on the network layer, particularly selective forwarding attacks.***

I. INTRODUCTION

A wireless sensor network(WSN) is one of the wireless networkswhich uselightweight, small wireless nodes deployed in distributed manner which are defined as sensors to monitor the conditions of theenvironmental system. WSN is widely used in the application areas of monitoring and surveillance and mainly focused on military and environmental monitoring (eg. health, waste water, industrial) which is designed for data collection and analysis in real time. Sensor subsystem, processing subsystem and communication subsystem are used in every sensor node for sensing the data from the node, performing computation using the collected information and exchanging message with the neighboring nodes respectively.

In WSN the transmission range between the nodes is limited while sending the packets from source to destination and it needs many hops distance to reach its destination which is one of the loophole. Complex computations and the need of more memory for nodes are also some drawbacks. It is mandatory for a WSN to meet the expectations without compromising the security properties like integrity, confidentiality, availability and authentication. Various attacks involved in WSN are sybil, warm hole, impersonation, eavesdropping, traffic analysis and SFA.

Packet drop attack(black hole attack) is one kind of denial of service attack which makes the data unavailable to the intended users. Packets which are supposed to forward are periodically dropped which makes loss of data.It is difficult to detect this attack and also preventing it. Dropping the packets of data occur for a particular time in the particular network by amischievous router which acts as malicious node in the sensor network.

It is easy to detect black hole attack rather than grayholeattack because in gray hole all the packets are dropped by the mischievous router by noticing the loss of packets as very large. In this paper, we have discussed about selective forwarding attack in WSN.In section 2 we analyzed the various schemes and methodologies which involves in the process of detecting and mitigating the SFA.In section 3 the latest Syed et al [11]'s IDS is described and we have only focused on SFA attack and proposed a new scheme to mitigate that attack.

II. RELATED WORK

YuB and Xiao[2] proposed a scheme where few nodes are acting as checkpoints in the path of data transmission; acknowledgments will be generated after receiving the packets of data. To mitigate unusual loss of data packets, acknowledgments ensure an authenticated communicationwithout loss. If there is occurrence of loss, one warning message will be sent so that communication will be terminated. Depending upon the acknowledgments, attacks can be analyzed.

Jiang and Zhang's scheme [6] uses trust and loss of packetsas the heuristic features for their scheme. When transmitting data from source to destination, the intermediate nodes are used to detect the loss of data and how much data is lost. Those intermediate nodessendreport to the base station which controls all the nodes. Attack node is defined by the level of trust and how loss of data is occurred.

Heterogeneous Sensor Network model is proposed in Brown and Xiaoping's scheme [3] which has two types of sensors which are high end sensors and low end sensors. These H sensor and L sensor are deployed in as different clusters where cluster head is mainly used as a base station. Cluster Head acts as a gateway between two different clusters and ensures the transmission as secure and efficient.

Sophia Kaplantzis et al [1] proposed scheme in which support Vector machines and sliding windows are utilizedfor mitigating the selective forwarding attack. Instead of using central station here SVMs are used which monitor the uncertain dropping of data packets from the source node to the destination. It increments the accuracy of detecting attack and make the communication in secure manner.

A light weight defense scheme was proposed by Xin etal[5] in which neighboring nodes are acting as monitoring nodes. Each node monitors other node so that loss of data packets are easy to detect and selective forwarding attack will be mitigated.Mızrak et al [4] analyzes the existing methodswhere a static user-defined threshold, which is fundamentally limiting, whereas they used a compromised router detection protocol works dynamically which is based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur.Focusing on adhoc networks Saraswati Mukherjee et al [7] use two phases to detect selective forwarding attack in their scheme and they proposed an algorithm with more efficiency. In first phase cluster head is used to find attack where as in second control packets are used.

In recent, Eliana and Andreas [8] proposed a scheme which uses directional antennas to detect the attack and countermeasure is provided for that. Node reliability estimator is used in Biru and Shanchieh's [9]scheme. That scheme eliminates mischievous nodes by monitoring their parent nodes. New routing algorithm is proposed to maintain zero overhead and sensor rank is used to determine the critical sensor node.

Sunhoand Lauren [10] proposed Hop by hop co-operative detection scheme which first analyzes the malicious scenarios and then find the misbehavior and tries to increase the probability for delivering the data packet without loss.Syed et al [11] proposed an Intrusion Detection System (IDS) which is based on trust values which is the latest scheme. For forwarding packets trustworthy nodes are identified by using the trust values. Trust is obtained based on the direct observation of the node.

III. EXISTING SYSTEM

In earlier various schemes are used to detect and mitigate selective forwarding attackin order to ensure secure transmission from source node to the destination node of the WSN as discussed in the Literature Survey chapter.WSN needs a low computation cost and highly secured Intrusion Detection System (IDS) for detecting and mitigating the vulnerable scenarios and attacks.

Syed et al[11]'s Intrusion Detection System (IDS)is one among them which is used to detect the attacks related to WSN like Hello flood attack, jamming attack and selective forwarding attack by using the trust values. This scheme contains a trust manager which is used to maintain direct and indirect trust of the nodes. Risk factors are analyzed and updated. Based on the status of the nodes, attack is identified.

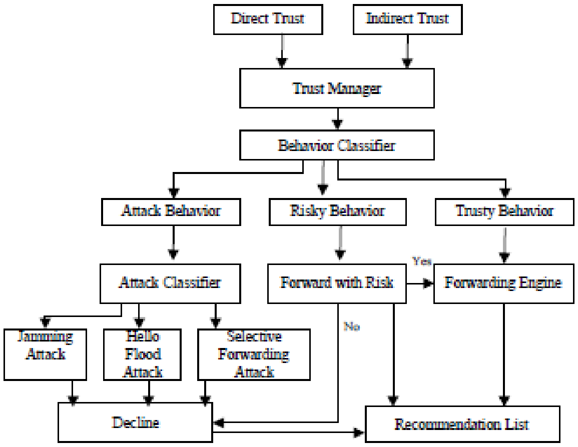


Fig 1. Existing System

To detect the selective forwarding attack, the ratio between packets forwarded and packets received are analyzed to define the successfully packet forwarded within particular period of time.

IV. PROPOSED ARCHITECTURE

Existing system provides resistance to Hello flood attack, jamming attack and selective forwarding attack. Our proposed system focuses on providing resistance to selective forwarding attack which is highly vulnerable. In our proposed every node in the network is enabled to monitor the traffic of the entire network and also considering the risk factors.It is important to resist the attack by providing remedies to the security loophole of the system.

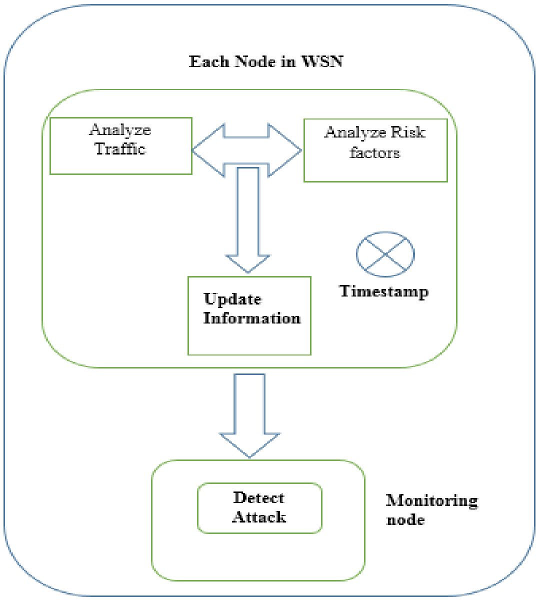


Fig. 2 Proposed Architecture

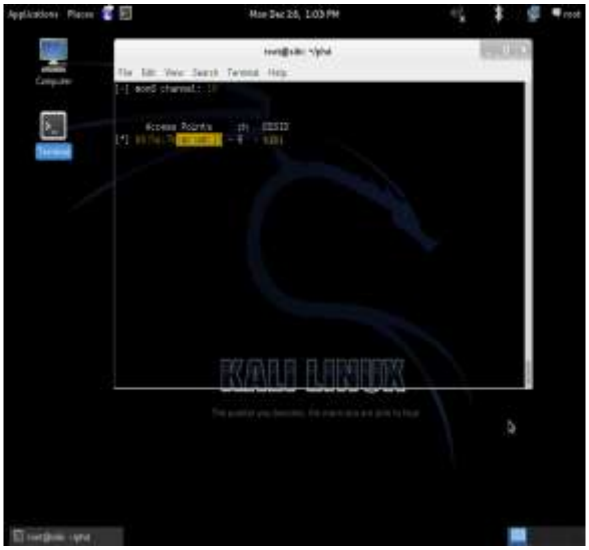
Additionally time stamp is added to avoid the loss and it is easy to detect the attack if the forwarded packets exceed the time stamp. At each time forwarding packets from source to the destination node each node analyze the risk factors and traffic and then update all those formation by self.

Then monitor node find whether there are loopholes with those updated information from each nodes. If there is variance in the traffic then attack is made with those nodes.

V. IMPLEMENTATION RESULT

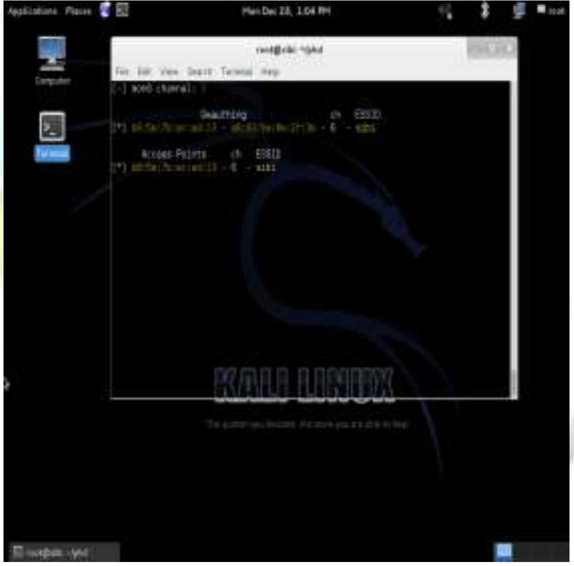
Kali Linux which is a debian based advanced penetration testing Linux distribution used to implement the attack. Attack is implemented in real-time with mobile connected wifi network.Here the valid user is authenticated in which he is obtained with his correct credentials. By this scenario attack is implemented for real-time.

The valid user is identified by his IP address and after that authentication is done by changing his Wifi hotspot status from connected to disconnected.



```
[-] mon0 channel: 10

      Access Points     ch   ESSID
[*] [illegible] - 6 - sibi
```

Fig.3. Identifying valid user

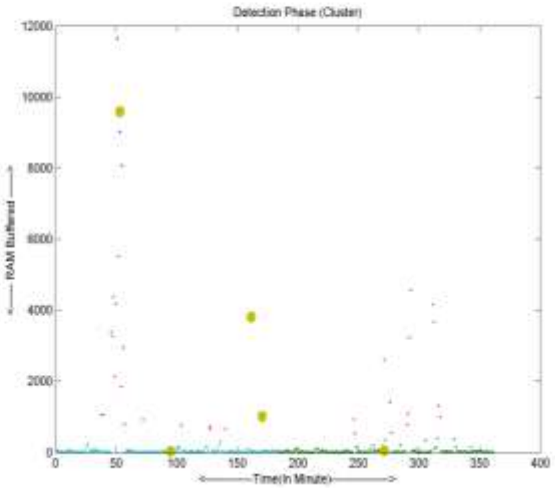


```
[-] mon0 channel: 6

                  Deauthing                  ch   ESSID
[*] [illegible] - [illegible] - 6 - sibi

      Access Points     ch   ESSID
[*] [illegible] - 6 - sibi
```

Fig.4. Deauthenticating valid user

Seeing the implantation result, Fig.3 shows that the attacker identifying the valid user's IP address and then the process of authentication of that valid user is depicted in Fig.4 which clearly shows that attack is performed by the attacker.

In the below graph the detection of attack is shown where x axis defines time in minutes and y axis defines size of RAM buffered in that time. The green colored dots denote the occurrence of attacks.



Attack

Fig.5 Detection of attack

VI. CONCLUSION

Thus in this paper we have proposed a scheme in which will detect to selective forwarding attack to ensure the secure transmission in Wireless Sensor Networks. In our scheme each node analyze the secure factors, update and forward them then monitor node detects attack if available. In future the scheme for mitigating the selective forwarding attack will be implemented without compromising the security factors.

REFERENCES:

[1] S. Kaplantzis, A. Shilton, N. Mani, and Y.A. Sekercioglu. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on, pages 335 –340, 2007

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

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

[4] Mızrak, Alper T., Stefan Savage, and Keith Marzullo. Detecting malicious packet losses Parallel and Distributed Systems, IEEE Transactions on Parallel & Distributed Systems, vol.20, no. 2 ,2009.

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

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

[7] Saswati Mukherjee et al, “Detection of selective forwarding attacks in Wireless Adhoc Networks using Binary Search”, Third International Conference on Emerging Applications of Information Technology (EAIT), 2012.

[8] Eliana Stavrou and Andreas Pitsillides, “Recovering from the selective forwarding attack in WSNs”,IEEE,2014

[9] Biru Cui and Shanchieh Jay Yang, “ NRE: Suppress selective forwarding attacks in WSN”,IEEE, 2014

[10] SunhoLimand Lauren Huie, “Hop by hop co operative detection of selective forwarding attacks in energy harvesting WSNs”, IEEE International conference on computing(ICNC),2015

[11] Syed Muhammad Sajjad, SafdarHussainBouk, Muhammad Yousaf, “Neighbor Node Trust Based Intrusion Detection System for WSN”, Procedia Computer Science 63 (2015) 183 – 188.