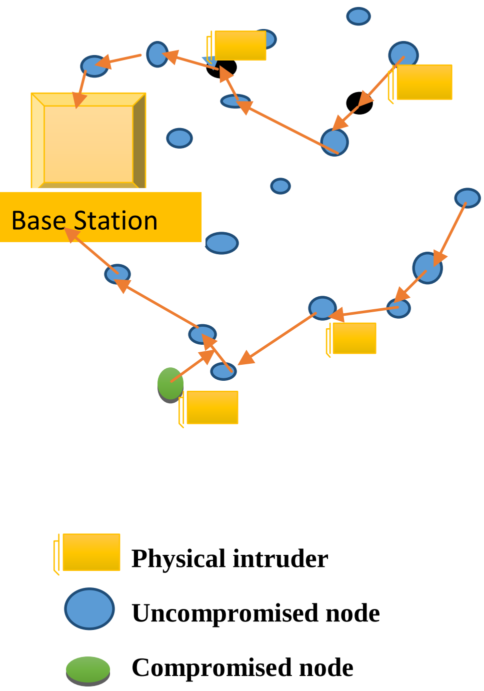
WIRELESS SENSOR NETWORK ON SELECTING FORWARDING ATTACK: A SURVEY

Anshul

Department of Software Engineering

UIET,MDU University,Rohtak, Haryana, India

Abstract: A Wireless Sensor Network (WSN)is a network made of numerous small independent sensor nodes which sense the network by detecting events in the surrounding environment.. The Sensor Networks suffer from various security threats like (i)sink hole attack, (ii) black hole attack, (iii) wormhole attackand (iv) selective forwarding attacks (5)smurf attack.Selective forwarding attacks corrupt some missioncriticalapplications such as battlefield surveillance, forestfire monitoring and military monitoring system. In these attacks, corrupted or malicious nodes behavelike normal nodes in most time but selectively dropsensitive packets.The compromised node attempts to disrupt the normal communication process by selectively dropping the certain packets while forwarding the others.Such selective dropping is hardto detect. In this paper we have described all theexisting defensive schemes according to our best knowledgeagainst this attack and getting a better understanding related to this attack and its complete workingscenario.**Fig1**. An example of selective forwarding attacks.



Keywords

Wireless Sensor Network, Selective Forwarding Attacks, Compromised Nodes, threats, Denial of Service (DoS)

I. Introduction

In Selective Forwarding Attack, internal nodes that are compromised selectively will be forwards some ofthe packets passing through them. If any node drops all the packets, then it will be becomes black hole attack. Therefore,selective forwarding attack is sometimes called as a special case of black hole attack.

Attacks against wireless sensor networks(WSN) could be broadlyconsidered from two different levels of views.

1. The attack against routing mechanisms.
2. The attack against security mechanisms.

Attack Models

Many security attacks are present in Wireless Sensor Networks
and they are,

1. Dos attack
2. Black hole attack
3. Sink hole attack
4. Wormhole attack
5. Selective forwarding attacks.
6. Sybil attacks
7. Node replication attacks
8. Hello flood attack

The main objective of this paper is to give an overview of different techniques which will be able to prevent Selective Forwarding Attack. Thispaper is organized as follows: Section 2 present theoverview of selective forwarding attack and its types.Section3 classifies the detection technics of SelectiveForwarding attack. Section4 gives the little bit information about prevention technics of Selecting Forwarding Attack.The final section concludes this paper.

II. Overview of Selective Forwarding Attack

The Selective Forwarding attack, a special case of denial of service(Dos) attack, was first defined by Karlof as "malicious nodes behaves like black hole and may refuse tos forward certain messages and simply drop them, ensuring that they are not propagated any further." It is normally assumed that the intermediate nodes, in multihop sensor networks,it is participating in the communication process between the source and the sink, faithfully forwarded the messages that they receive from the other nodes. In the Selective forwarding attack, also known as Grayhole attack,in this case the compromised node attempts to disrupt the normal communication process by selectively dropping the certain packets while forwarding to the others. The adversary may choose to drop the packets originating from the particular node or multiple nodes, thus causing the denial of service for that node(s) or the packets of a particular type. The selective forwarding attack can be launched as inside attack by compromising a legitimate node within the network to drop the subset of packets while forwarding the others. To be more effective, the adversary tries to place itself on the actual data flow path between the two communicating nodes such as this will help to get more traffic. Because of limited transmission range, sensor networks forwards these packets to the base station in multihop manner and while being routed to the base station packets may be dropped because of collision, congestion or any other network problems. The selective forwarding attack exploits these network problems and thus it will becomes more difficult to detect.

2.1. Types of Selective Forwarding Attack:

In the original form of the selecting forwarding attack, the compromised node attempts to disruptedcommunication between the communicating nodes by dropping certain packets of interest while forward the others. The Table 1 below describes the other forms of selective forwarding attack:

Table 1: Types of Selective Forwarding Attack

Name	Description
Blackhole attack	Compromised node drops every packet it receives; also it may forward the packet to wrong path creating unfaithful routing information in the network.
Neglect and Greed	Compromised node arbitrarily neglects to forward certain packet but still acknowledge the reception of data to the sender. When the node gives priority to its own messages, it becomes greedy, thus dropping the packets received from the other nodes and forwarding its own messages.
Blind Letter Attack	With arbitrarily malicious nodes in the network, it should be guaranteed that the next node to which the relay node forwards the packet is actually a legitimate neighbor of the current relay node.

Besides the above described types, the malicious sensor node involved in launching the selective forwarding attack may delay the forwarding of the packets to the next hop to create the confused routing information.

2.2 Different Forms of Selective Forwarding Attack

There are some different forms of selective forwarding attack.In the First form of the selective forwarding attack, the compromised node drops some packets. In the Second form, the Selective forwarding attack behaves like a Black hole, in which the message is forwards to the wrong or incorrect path, creating false routing information in the network. Third form of selective forwarding attack delays packet passing through the network generating confused routing information between sensor nodes.

3. Classification of Schemas Against Selective Forwarding Detecting:

The schemes for defending or protecting against selective forwarding attack can be classified according to the two types of criteria i.e. nature of scheme and defense scheme.The nature of scheme can be classified into two classes i.e. centralized and distributed.Defense of scheme can again be classified into two classes, detection based and prevention based.

A. Detection and Preventions:

Detection based schemes are detect the malicious node or the attack or both. On theother hand the prevention based schemes only ignores the nodes or by pass the malicious node and are not capable of detecting the malicious nodes and the attack.

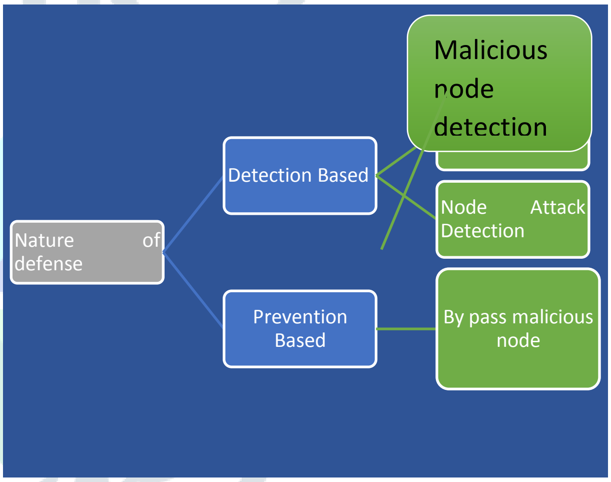


Figure 2. Classification by defense of schemes

B. Distributed and Centralized

In Distributed based schemes, both sensor nodes and base stations are responsible for prevention and detection of the malicious nodes and selective forwarding attack.On the other hand,the centralized based schemes only base stationor cluster head are responsible for countering the selective forwarding attack.

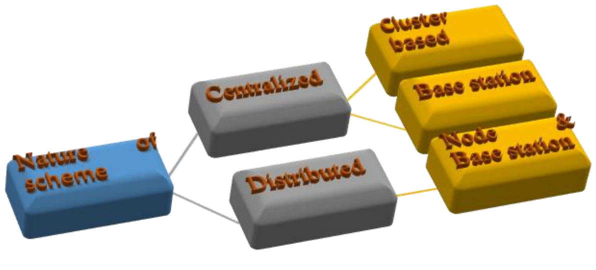


Figure 3. Classification by nature of schemes

3.1 Attack Defensive Technics:

Many techniques are introduced by several researchers to detect malicious nodes that cause selective forwarding attack in Wireless Sensor Networks.There are many detecting technics by which many researchers are trying to remove the complexity which is generated by Selecting Forwarding Attack. In the existing Defensive technique algorithm, a single static path is created for sending the packets to the sink node in the network.When an attack is identified, server removes the malicious node and the packets are retransmitted through the new shortest path without losing the connection.

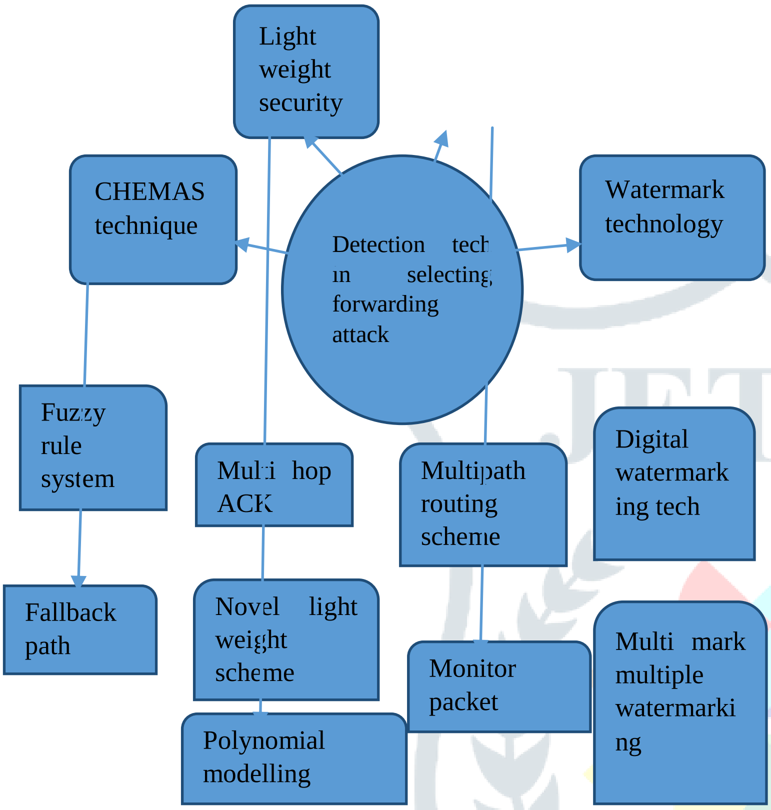


Figure 4: Classification of Selective Forwarding Attack Techniques

3.1.1 Defense Mechanism

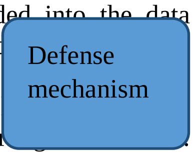
This Defensive techniqueconsists of three phases for secure information delivery. In first phase the node firstly discovers a path and its neighbor nodes also, in the second phase, data is propagated in a multipath, it require tochecks whether the received data is correct or not, and in the final phase if any error is detected then a MONITOR packet is generated and then the malicious node is removed.

3.1.2 Lightweight Defense Scheme

Lightweight security scheme is used to detect selective forwarding attack using multi hop acknowledgement technique or scheme to launch alarms by obtaining responses from intermediate nodes.. This scheme allows both the base station and source nodes to collect attack alarm information from intermediate nodes.Each node in the forwarding path is incharge of detecting malicious nodes. If an intermediate node detects a node as malicious in its downstream/upstream, then it will send an alarm packet to the source node/base station through multi-hops. Downstream denotes direction towards base station and upstream denotes direction towards source node. The detection process consists of upstream detection and downstream detection.. In the other words, though the base station is deafened by malicious node so the source node can make decisions and responses. The scheme can efficientlyobtain those alarm information whenever intermediate nodes in packet forwarding path detect any malicious or corrupted packet dropping.

3.1.3 Watermark Technology

In the digital watermarking technology is used to calculatethe rate of packets which is dropped and modified. Each sensor node can send only a few data bits at a time and by this the length of watermark embedded into the data should be very short. The source noc watermark W with key K and feature of Then the source node embeds or tightly ho into the original data and transfers it thr When the packets reach the BaseStation, then the Base Station obtains the feature of thepackets and generates the watermark W1 by watermark generation algorithm, then the Base Station extracts the watermark directly from the received packets by Watermark embedding algorithm denoted as W2; finally the packet modified rate is calculate by comparing the watermark W1 and watermark W2.



3.1.4 CHEMAS Technique

The Checkpoint Based Multi-hop Acknowledgement Scheme (CHEMAS) was developed by Bin Xiao et al., to detect the selective forwarding attack. When a message is generated by a source node and is delivered to the base station,then the checkpoint nodes are selected randomly. The base station and each checkpoint nodes generate theacknowledgement (ACK) message that is transmitted from the start node to the source node. ACK messages have the Time to Live (TTL) value, which is responsible for sets the hop count. If TTL becomes zero, ACK message is dropped and an alert message is sent to the source node. If any particular node does not send ACK message to the source node then it is identified as the compromised node. Then the source node sends an alarm message about the compromised node to the base station. Another technique for the Checkpoint Based Multi-hob Acknowledgement Scheme (CHEMAS) to detect the compromise nodes that perform a selective forwarding attack when sensing data transmission. If more number of check nodes is presented, then the checking time of the packet transferred will increase and so there will be a time delay in reaching the destination.

4. Selective Forwarding attack prevention:

Multipath routing can be used to counter the selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

Conclusion:

Secure and safe and on time transmission of packets is the basic need in wireless sensor network. One of the attacks that distract this need is Selective Forwarding attack. This paper presents a brief overview of the selective forwarding attack and its working.In this paper also describes the detection measures against it in the wireless sensor networks.

Refrences:

1. Geethu P C and Rameez Mohammed A, “Defense Mechanism against Selective Forwarding Attack in Wireless Sensor Networks”, Conference on Computing, Communications and Networking Technologies (ICCCNT), July 2013, pp. 1-4
2. Sushil Sarwa and Rajeev Kumar, “Wireless Sensoe Network in Selective Forwarding Attack”,World Academy of Science, Engineering and TechnologyInternational Journal of Computer, Control, Quantum and Information Engineering Vol:7, No:7, 2013
3. J. Anne Shirley1, J. John Raybin Jose2,International Journal of Scientific Engineering and Research (IJSER) www.ijser.inISSN (Online): 2347-3878
   Volume 2 Issue 6, June 2014
4. Jaspreet SinghDepartment of Computer Science Engineering, RIMT IET, Punjab, India &Anuj GuptaHead, Department of Computer Science Engineering,RIMT IET, Punjab, India”Different Approaches to Mitigate Selective Forwarding Attacks in WSN”Volume2 Issue 4 ,Augeust 2014
5. Preeti Sharma1,Monika Saluja2 and Krishan Kumar Saluja3“A REVIEW OF SELECTIVE FORWARDING ATTACKS INWIRELESS SENSOR NETWORKS”International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.3, July 2012
6. Leela Krishna Bysani Dept. of Computer Science and Engg. National Institute of Technology Rourkela” A Survey On Selective Forwarding Attack in Wireless Sensor Networks”International conference of device and communications ,(ICDeCom)24-25 february,Mesra,India.
7. Wazir Zada Khan Yang Xiang Mohammed Y Aalsalem Comprehensive Study of Selective ForwardingAttack in Wireless Sensor Networks *I.J. Computer Network and Information Security*, 2011, 1, 1-10
8. Ahmad Salehi S., et al., *“Detection of Sinkhole Attack in Wireless Sensor Networks”* Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, pp 361-365.
9. Tejinderdeep Singh and Harpreet Kaur Arora, *“Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool”,* International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013, pp 32-35.
10. Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj *“Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET ”* International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.1737-1741
11. Vikash Kumar1, Anshu Jain2 and P N Barwal3” Wireless Sensor Networks: Security Issues, Challenges andSolutions” International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868 © International Research Publications House http://www. irphouse.com
12. K.Venkatraman,,J.Vijay,Daniel,G.Murugaboopathi”Various Attacks in Wireless Sensor Network: Survey” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013
13. Suchitha Patil, Dr.B.B. Meshram, “Network Intrusion Detection and Prevention Techniques”, *International Journal of Scientific and Research Publications,* Volume 2, Issue 7, July 2012.
14. M. S. Islam, S. A. Rahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", *International Journal of Advanced Science and Technology*, vol. 36, (2011).
15. S. Boob, P. Jadhav, "Wireless Intrusion Detection System", *International Journal of Computer Applications,* vol. 5, no.8, (2010**)**, pp. 9-13.
16. R. S. Shirbhate and P. A. Patil, "Network Traffic Monitoring Using Intrusion Detection System", *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 2, no. 1. (2012).
17. I. Demirkol, F. Alag¨oz, H. Delic, and C. Ersoy, "Wireless Sensor Networks for Intrusion Detection: Packet Traffic Modeling*", IEEE Communication Letters,* vol. 10, no. 1, (2006), pp.22-24.
18. Y. Ponomarchuk, and D.-W. Seo, "Intrusion Detection Based on Traffic Analysis in Wireless Sensor Networks*", Proceedings of the 19th annual IEEE Wireless and Optical Communications Conference,*(2010)May 14-15; Shanghai.
19. M.D. Aime, T. Politecnico, G. Calandriello and A. Lioy, "A Wireless Distributed Intrusion Detection System and a New Attack Mode*", Proceedings of the 11th IEEE Symposium on Computers and Communications,*(2006)June 26-29.
20. J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, Botnet,“Classification, Attacks, Detection, Tracing, and Preventive Measures”, *EURASIP Journal on Wireless Communications and Networking,* vol. 2009, Article ID 692654, 11 pages, 2009.
21. B. Yu and B. Xiao, “CHEMAS: identify suspect nodes in selective forwarding attacks,” in Journal of Parallel and Distributed Computing, Vol. 67, No. 11, 2007, pp. 1218-1230
22. S. Kaplantzis, A. Shilton, N. Mani and Y. Sekercioglu, “Detecting selective forwarding
    attacks in wireless sensor networks using support vector machines,” in 3rd Conf. of Intelligent Sensors Sensor Networks and Information Processing, Dec. 2007, pp. 335-340.
23. Hae Young L, Tae Ho C. Fuzzy-based reliable data delivery for countering selective forwarding in sensor networks. Hong Kong, China, Springer-Verlag, 2007, p. 535-544.
24. Tran Hoang Hai, Eui-Nam Huh, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge” Seventh IEEE International Symposium on Network Computing and Applications, 2008, pp.325-331.
25. Huijuan Deng, Xingming Sun, Baowei Wang, Yuanfu Cao ,‘Selective Forwarding Attack Detection using Watermark in WSNs” International Colloquium on Computing, Communication, Control, and Management (2009 ISECS), pp.109-113
26. S.-B. Lee and Y.-H. Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN’06), pp. 59-70, 2006.
27. Guorui Li, Xiangdong Liu, and Cuirong Wang, “A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks”, pp.554-558, 2010.
28. Xie Lei, Xu Yong-jun, Pan Yong, Zhu Yue-Fei1 ,“A Polynomialbased Countermeasure to Selective Forwarding Attacks in Sensor Networks” International Conference on Communications and Mobile Computing, 2009, pp.455- 459.
29. C.Tumrongwittayapak and R. Varakulsiripunth, “Detecting sinkhole attack and selective forwarding attack in wireless sensor networks,” 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), (2009), pp. 1-5.
30. L. Coppolino, S. D’Antonio, L. Romano and G. Spagnuolo, “An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies”, 2010 5th International Conference on Critical Infrastructure (CRIS), (2010), pp. 1-8.