Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.45 – 50

A Survey on Selective Forwarding Attacks in Wireless Sensor Networks

Jyoti Shokeen[1], Palak[2], Preeti Devi[3]

[1]Department of Computer Science and Applications, MDU Rohtak, India

[2]Department of Computer Science and Applications, MDU Rohtak, India

[3]UIET, MDU Rohtak, India

[1] jyotishokeen12@gmail.com; [2] palak.aug6@gmail.com; [3] prtbrk@gmail.com

Abstract— Wireless sensor network has become an emerging technology due its wide range of applications in object tracking and monitoring, military commands, smart homes, forest fire control, surveillance, etc. Wireless sensor network consists of thousands of miniature devices which are called sensors but as it uses wireless media for communication, so security is the major issue. There are number of attacks on wireless of which selective forwarding attack is one of the harmful attacks. This paper describes selective forwarding attack and detection techniques against selective forwarding attacks which have been proposed by different researchers. In selective forwarding attacks, malicious nodes act like normal nodes and selectively drop packets. The selective forwarding attack is a serious threat in WSN. Identifying such attacks is very difficult and sometimes impossible. This paper also presents qualitative analysis of detection techniques in tabular form.

Keywords- wireless sensor network, attacks, selective forwarding attacks, malicious nodes.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a heterogeneous system consisting of spatially distributed ad-hoc sensors that are capable of processing, gathering sensitive information and communicating the information with other nodes in the network [1]. Sensor node sense the real world physical conditions such as sound, temperature, humidity, pressure, etc at different location. The sensor can send the command or queries to the base station which ultimately forwards those commands or queries into the network. WSN's are vulnerable to many types of attacks such as DoS attacks, selective forwarding attacks, Sybil attack, wormhole attack, etc. due to unsafe and unprotected nature of the communication channel, untrusted and broadcast transmission media, therefore security is a vital requirements for these networks. An adversary can compromise a sensor node, alter the routing path, waste network resources, eavesdrop on messages, and inject false information. A common attack in WSN is DoS attack [2]. A number of DoS attacks against wireless sensor networks have been identified such as selective forwarding attack, hello flood attack, wormhole attack, black hole attack and sinkhole attack [3, 5, 8 and 9]. This paper describes the selective forwarding attack which is quite simple to implement. Selective forwarding attacks may corrupt some mission critical

applications such as military surveillance. In these attacks, malicious nodes work as normal nodes in most time but selectively drop some packets which are hard to detect. This paper describes various techniques to detect selective forwarding attacks and qualitative analysis of different detection techniques.

II. RELATED WORK

In this paper we will focus on selective forwarding attacks. Selective Forwarding Attack is one of the network layer attacks [6, 13]. In multi-hop WSN, the nodes send packets to the neighboring nodes assuming that they forward the packets to destination faithfully [3]. In a selective forwarding attack, malicious nodes may refuse to forward some messages and just drop them to ensure that they are not further propagated. When a node refuses to forward every packets it sees then it is a black hole. A more refined of this attack is when an adversary node selectively drops/forwards certain packets. The malicious node interested in modifying or suppressing packets can reliably forward the remaining traffic to make her less suspicious. Selective forwarding attacks are considered most effective when the attacker is included on the data flow path explicitly [5, 6 and 10].
Fig.1. [3] shows how number of ways an adversary can deploy malicious nodes in transmission path to Base Station.

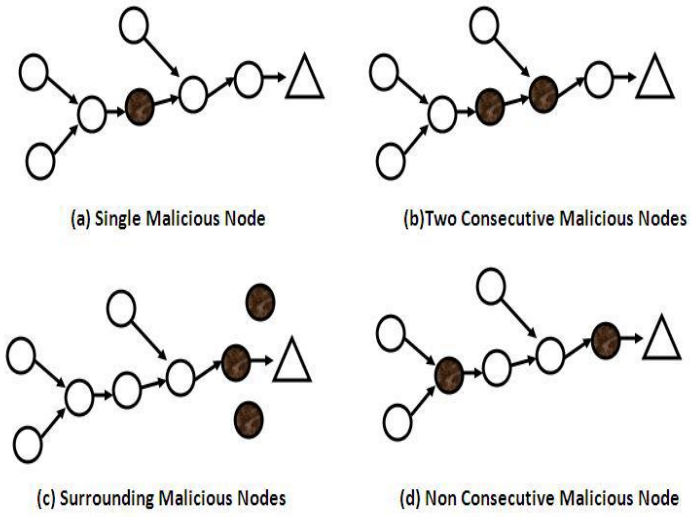

Fig. 1 Categorization of Selective Forwarding based on node count in WSN

III. CLASSIFICATION OF THE SCHEMES FOR SELECTIVE FORWARDING DETECTION AND COUNTERMEASURES

On the basis of defense against selective forwarding attack, we can classify the scheme according to nature of scheme and defense of scheme. The nature of scheme can be further classified into distributed and centralized schemes. Defense of scheme can be classified into detection based and prevention based classes.

A. Distributed and Centralized

In Distributed based schemes, it is the responsibility of sensor nodes and base stations to detect and prevent the selective forwarding attack and malicious nodes. While base station or cluster head is only responsible for countering the selective forwarding attack in centralized based schemes.

B. Detection and Preventions

Detection based schemes can detect the malicious nodes or the attack or both. On other hand the prevention based schemes ignores the malicious nodes not capable of detecting the attack and adversary nodes.

IV. PROPOSED DETECTION TECHNIQUES OF SELECTIVE FORWARDING ATTACKS

An overview of the existing schemes and techniques in opposition to selective forwarding attack is described below.

4.1. Yu et al. [3, 11] proposed a distributed detection technique in which multi hop acknowledgements are received from intermediate nodes. The approach launches alarms by receiving responses from intermediate nodes. Each node in the forwarding path is responsible for detection of malicious nodes. On the detection of a node as malicious in downstream/upstream by any intermediate node, an alarm packet is sent to the base station or source node via multi-hops.

4.2. Karlof et al. [12] suggested that Multi-path routing can be used to detect selective forwarding attacks. The messages sent over n paths where nodes are completely disjoint are fully protected against selective forwarding attacks that may involve at most n compromised nodes. Use of multiple braided paths provides probabilistic protection against selective forwarding by using localized information only. Nodes are allowed to dynamically choose the next hop for packet from a set of nodes, thereby reducing the chances of an adversary to gain full control of a data flow.

4.3. Xiao et al. [2, 13] have proposed a technique CHEMAS (checkpoint-based multi-hop acknowledgement scheme) to identify suspected nodes in the network. In this scheme some part of intermediate nodes is randomly selected in the forwarding path as checkpoint nodes that are responsible for generating acknowledgements for each packet received. In addition each node needs a one-way hash key chain for ensuring the authenticity of packets. Delay mechanisms are also developed to send current one-way hash key. Each intermediate node in a forwarding path is capable of detecting abnormal packet loss and identifying suspect nodes on not receiving enough acknowledgements from the downstream checkpoint nodes.

4.4. Hung-Min Sun et al. [14] proposed a multi data flow topologies (MDT) method to countermeasure the selective forwarding attack. In this scheme the sensor nodes are divided into two-dataflow topologies, both of which can cover the monitored area, therefore the base station only requires one report from either topology to control the entire network. If a malicious node exists in one topology, the base station can still obtain packets from other topology. Sensor nodes may locate in a range of some regions. When the base station loses some packets, it will mark all possible regions that the malicious sensor nodes may be deployed in and thus the base station can utilize the information to locate the malicious sensor nodes.

4.5. Sophia Kaplantzis et al. [15] proposed a scheme based on Support Vector Machines (SVMs) and sliding windows. This centralized intrusion detection scheme can detect selective forwarding attacks and black hole attacks without depleting the energy of nodes and with high accuracy. Routing information local to the base station is used in the network and alarms are raised on the basis of the 2D feature vector (bandwidth, hop count).

4.6. Hea Young et al. [16] proposed Fuzzy based reliable data delivery scheme for countering selective forwarding attack which is an improved form of Multipath routing method. The enhancement is that the number of transmission path varies with number of attacker. Using the number of malicious nodes and energy level of the network, fuzzy logic is used to determine the number of paths for data. If multi-path routing is insufficient for reliable data delivery, the propagation limiting method is used as a means for routing in the scheme.

4.7. Jeremy Brown et al. [18] proposed an approach to detect selective forwarding attack using a Heterogeneous Sensor Network (HSN) model. The HSN consists of powerful high-end sensors (H-sensors) and large number of low-end sensors (L sensors) and is based on the Sequential Probability Ratio Test (SPRT) method [23]. The simulations results show that the proposed scheme achieves high detection ratio and very low false alarm rate. A simple method of detecting whether a downstream node has properly forwarded a packet is to passively listen for the transmission. If a node in the path drops the packet, the upstream node (farther away from the cluster head) will observe the packet drop. The monitoring node (L-sensors) will include the node ID of the dropper in the packet to report the packet drop, and then will transmit the packet to the cluster head (H-sensor).

4.8. Xingming Sun et al. [19] et.al proposed a digital watermarking technology to detect selective forwarding attacks to verify the authenticity and reliability of data. In this method, watermarking information is generated and embedded at source sensor

nodes side, whereas watermarking extraction and its verification are performed at base station side. On the basis of packet loss rate from received data, the Base station will judge if there are malicious nodes in the transmission path. The scheme can precisely detect if malicious nodes have modified or discarded the contents of the packets.

4.9. Young Ki Kim et al [10] proposed a centralized based detecting scheme called CADE (Cumulative Acknowledgement based Detection) of selective forwarding attacks, which identifies malicious nodes delivering selective forwarding attack without the need for time synchronization. The scheme also provides security against sinkhole attack. Their scheme sends cumulative acknowledgments to the base station. CADE consists of three phases: Topology construction and route selection, data transmission and detection process. SEEM [22] protocol is used for topology construction and route selection.

4.9. Xin, et al. [22] proposed a light weight defense approach against selective forwarding attack that is based on hexagonal WSN mesh topology and uses neighbour nodes as the control or monitor nodes. The neighbour nodes are responsible for monitoring the transmission of packet drops and to resend the dropped packets.

Table 1. Qualitative analysis of Detection Techniques

Technique	**Type (Detection/ Prevention)**	**Scheme Nature**	**Pros and Cons**
Yu and Xiao's Technique [11]	Detection	Distributed	1. Launch alarms by receiving response by intermediate nodes. 2. Increases cost of the network. 3. Detection accuracy is 95% even when the channel error rate is 15%. 4. Sensor nodes take much effort to detect the selective forwarding attack.
Karof et al's Scheme [12]	Prevention	Distributed	1. Reduce chances of an adversary to gain complete control of a data flow. 2. Increase in energy consumption when the number of paths increases. 3. Increase in Network flow and communication overheads. 4. Fails if nodes around the base stations are compromised
CHEMAS [13]	Detection	Distributed	1. Using one-way hash key chains for authentication for each packet requires storage space. 2. Detect abnormal packet loss and identify suspect nodes, if checkpoint node does not receive enough acknowledgements. 3. More energy is consumed by sending acknowledgement. 4. No guarantee for reliable transmission of packet. 5. It requires nodes to be loosely time synchronized.
Hung-Min Sun et al's scheme [14]	Prevention	Centralized	1. The scheme is lightweight and simple. 2. Sensor nodes can detect and identify the malicious sensor nodes in less effort. 3. Dropped packets need not to be re-sent to detect malicious sensor nodes. 4. The scheme can defend several kinds of attacks. 5. Scheme cannot identify compromised nodes efficiently. 6. Sending of duplicate packets increases communication overhead.
Support Vector Machine Based Technique [15]	Detection	Centralized	1. Detect black hole attacks with 100% accuracy and selective forwarding attacks with 80% accuracy. 2. No expansion of sensor node's energy as intrusion detection is performed in the BS. 3. Suffer from single node failure problem. 4. Does not identify malicious nodes or find alternative paths.

Fuzzy-Based Reliable Data delivery [16]	Prevention	Distributed	1. Improvement form of Multipath routing method. 2. Number of attackers must be determined in advance. 3. Unnecessary consumption of redundant transmission of packets and scarce energy. 4. This scheme cannot identify compromised nodes and increase communication overhead.
Two hops Neighbor Knowledge [17]	Detection	Distributed	1. Effective even in high probability of collisions in WSNs. 2. Consume less energy by using over-hearing mechanism to reduce the transmission of alert packets. 3. Scheme would not be effective if the topology changes as it is assumed as static. 4. No countermeasure is proposed if the monitoring node is compromised**.**
Jeremy Brown et al's scheme [18]	Detection	Centralized	1. Better performance and security. 2. The scheme achieves high detection ratio and very low false alarm rate. 3. Single node failure problem in case if the cluster head is compromised. 4. No mechanism is proposed for reliable retransmission of drop packets.
Digital watermarking Technique [19]	Detection	Distributed	1. Can effectively detect if malicious nodes have modified or discarded packet contents. 2. Used to verify data authenticity and reliability in WSNs. 3. This method achieves 100% detection on packet forgery attack, selective forwarding, packet replay and packet tampering. 4. No data retransmission method is described after packet is dropped. 5. This scheme is unable to detect more than two malicious nodes in the path.
CADE [20]	Detection	Centralized	1. No need for time synchronization. 2. Scheme do not work if topology changes. 3. Suffer from single node failure problem. 4. Scheme is not energy efficient.
Chanatip's et al's scheme [21]	Detection	Centralized	1. Change in topology will affect the efficiency of the scheme. 2. Suffer from single node failure problem.
Wang Xin-sheng et al's scheme[22]	Detection	Distributed	1. Change in topology will affect the efficiency of the scheme. 2. No countermeasure is proposed if in case the monitoring node is compromised**.**

V. CONCLUSION

The primary need of the wireless sensor networks is the secure and timely transmission of packets in the network. This paper presents a brief introduction on selective forwarding attack in wireless sensor network and the way it affects the network. Then the different detection techniques used to counter the selective forwarding attack are discussed which would help the user to know the techniques which have been proposed by different authors and may help them to propose new one in the future. As an attack detection scheme itself cannot be an ultimate solution and prevention may be safer than relying on detection, it is of the essence that the techniques proposed in future should be enough competent so that they can both detect and prevent the selective forwarding attack.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *Communications Magazine IEEE,* Vol. 40, issue. 8, pp. 102–114, August 2002.

[2] Anthony D. Wood and John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", *IEEE* Computer, 35(10):54-62, October 2002.

[3] G.Padmavathi and D.Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" international Journal of Computer Security, Vol. 4, No. 1 & 2, pp. 117-125, 2009.

[4] Parida, Nachiketa Tarasia, Tulasi Ambasha Patnaik, "Security against Selective Forward Attack in Wireless Sensor Network", IOSR Journal of Engineering, Vol. 2(5) pp: 1200-1206, May. 2012.

[5] W. Z. Khan, Y. Xiang, and M. Y. Aalsalem, "Comprehensive study of selective forwarding attack in wireless sensor networks," International Journal on Computer Network and Information Security, vol. 1, pp. 1–10, 2011.

[6] Leela Krishna Bysani and Ashok Kumar Turuk, "A survey on selective forwarding attack in wireless sensor networks", Devices and Communications (ICDeCom), 2011 International Conference on. IEEE, 2011.

[7] Vinod Kumar Jatav, Meenakshi Tripathi, M S Gaur and Vijay Laxmi, "Wireless Sensor Networks: Attack Models and Detection," in *IACSIT Press, Singapore*, vol. 30, no.6.

[8] Kriti Jain and Upasana Bahuguna, "Survey on Wireless Sensor Network", *IJSTM,* Vol. 3 Issue 2, pp. 83-90, Sept 2012.

[9] Bharti Bains and Rohit Vaid, "Selective Forwarding based Intrusion Detection System for Secure Wireless Sensor Network," International *Journal of Computer Applications* 77(13):20-26, September 2013.

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

[11] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *AdHoc Networks (Elsevier)*, Sept, 2003.

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

[13] 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.

[14] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao, "An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks," in *Proc.3rd IEEE International Symposium on Security in Networks and Distributed Systems*, 2007.

[15] Sophia Kaplantzis, Alistair Shilton, Nallasamy Man, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines," 2007.

[16] Hae Young L and Tae Ho C. "Fuzzy-based reliable data delivery for countering selective forwarding in sensor networks", Hong Kong, China, Springer-Verlag, 2007, p. 535-544.

[17] Tran Hoang Hai and 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.

[18] Jeremy Brown and Xiajiang Du.,"Detection of selective forwarding attacks in heterogeneous sensor networks," in IEEE, vol. 1, 2008.

[19] Xingming Sun, Jianwei Su, Baowei Wang and Qi Liu, "Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks," in *International Journal of Security and Its Applications*, vol. 7, No. 4, July, 2013.

[20] Young Ki Kim, Hwaseong Lee, Kwantae Cho, and Dong Hoon Lee, "CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attacks inWireless Sensor Networks" Third International Conference on Convergence and Hybrid Information Technology, 2008, pp.416-422.

[21] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth, "Detecting Sinkhole Attack And Selective Forwarding Attack In Wireless Sensor Networks" ICICS 2009.

[22] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liangmin, "Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks' pp.226-232, IEEE, 2009.

