Security Mechanisms for Selective Forwarding Attack in Wireless Sensor Networks: Review and Analysis

Bhargavi Singh[1]
[1]*Research Scholar*

Abstract : *Wireless Sensor Networks have emerged as technology of the 21st century and provide powerful combination of distributed sensing, computing and communication. With its growing application areas, particularly in mission-critical applications such as military monitoring systems and battlefield surveillance, security has become an important need in order to protect the sensitive data involved. This necessity of effective and efficient security techniques to secure sensor networks has attracted a great deal of researchers' attention making it hot research area in the recent years. Among the number of attacks on the sensor network, the Selective Forwarding attack, alias Grayhole attack, is a serious and hard-to-detect security attack that can render the network useless if left undetected. In this attack, the main goal of the attacker is to prevent the important sensitive data from reaching the base station. To achieve this goal, the malicious node selectively drops certain packets, based on some chosen criteria, and forwards the remaining. The attack becomes more effective when the attacker includes itself on the path of data flow. This paper intent to give an overview and analysis of existing approaches to counter selective forwarding attack in wireless sensor networks.*

Keywords: *DoS, Grayhole Attack, Insider Attacks, Selective Forwarding Attack, Wireless Sensor Network*

I. Introduction

Wireless Sensor Networks have emerged as 'Modern Day Technology" attracting a great deal of researcher's attention. The recent advances in the low cost, low power devices and the radio technologies have stimulated the growth of wireless sensor networks with the widespread area of applications including the battlefield surveillance, military monitoring system, home automation, environment monitoring, healthcare monitoring and many more. Wireless sensor networks are application specific and consist of a large number of low cost, low power, resource constrained, tiny smart sensors, communicating using the wireless medium and are densely and randomly deployed with no fixed topology in remote and hostile locations. The sensor nodes are usually battery powered and possess very limited resources in terms of energy, storage, and processing capabilities. To sense, locally process the information and communicate it to the base station are the three key tasks of a sensor node. Besides providing the endless opportunities, the sensor networks also provide security challenges because of the sensitive data involved, limited battery and memory resources and unattended environment.

Sensor networks are vulnerable to a number of security attacks which can be either outside attack or inside attack [1]. Outside attacks are not very effective and not cause much damage to the network because they do not have the access to the network information. The inside attacks, on the other hand, are very effective and can disrupt the normal network functioning as the adversary is part of the network and has access to the network information. This makes it difficult to detect the adversary using traditional security mechanisms, authorization and authentication, as the adversary is legitimate member of the network. One such security attack on the sensor networks is the Selective Forwarding attack, a packet drop attack, launched with intention to suppress the important information reaching the base station. Such an attack is difficult to detect and is more effective when the attacker includes itself on the path of data flow from source to destination. The attack is mainly dangerous in case of mission critical applications and has the potential to disrupt the normal network operation and render the network useless. A number of security mechanisms have been proposed so far to counter the selective forwarding attack either by detection or by prevention. This paper layout an overview of the existing approaches to counter the attack. The paper also presents the analysis of the different security mechanisms. In view of the fact that the prevention schemes do not isolate the malicious node from the network and the threat exists, we mainly focus on the detection schemes in this paper.

II. Selective Forwarding Attack

The Selective Forwarding attack, a special case of denial of service attack, was first defined by Karlof [1] as "an attack where the malicious node refuses to forward certain messages and simply drops them ensuring they are not propagated any further." It is generally assumed that the intermediate nodes, in multihop sensor networks, participating in the communication process between the source and the sink, faithfully forward the messages they receive from the other nodes [1]. In the Selective forwarding attack, also known as Grayhole attack, the compromised node attempts to disrupt the normal communication process by selectively dropping the certain packets while forwarding the others. The adversary may choose to drop the packets originating from the particular node or a group of nodes, thus causing the denial of service for that node(s) or the packets of a particular type, for example, packet reporting the coordinates of the tank in battlefield. 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 as this will help to get more traffic. Because of the limited transmission range, sensor networks forwards the 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 other network problems. The selective forwarding attack exploits these network problems and thus becomes more difficult to detect.

2.1. Types of Selective Forwarding Attack:

In its original form the compromised node attempts to hinder the communication between the communicating nodes by dropping certain packets of interest and forwarding 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 [2]	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.

III. classification of existing security mechanisms

There are number of security mechanisms proposed to counter the selective forwarding attack in the wireless sensor networks which can be categorized as Prevention Schemes and Detection Schemes. The major goal of the prevention schemes is to deliver the packets to base station bypassing the malicious node and routing the packets through the multiple paths. This can be done using Multipath Routing [1], or Individual Path Forwarding [3] or by using Multi-Dataflow Topologies [4, 5]. As long as a path without the attacker exists within the network, the packet reaches the base station. These schemes do no attempt to isolate the malicious node but only try to avoid the packet loss. Since these schemes do not attempt to identify and isolate the malicious node, the threat still exists and so the need for the detection schemes. The detection schemes, on the other hand, attempts to identify the malicious node and to isolate it from the network by informing the other legitimate nodes about its presence. The detection schemes can be further categorized depending upon the techniques used to detect the attack within the network.

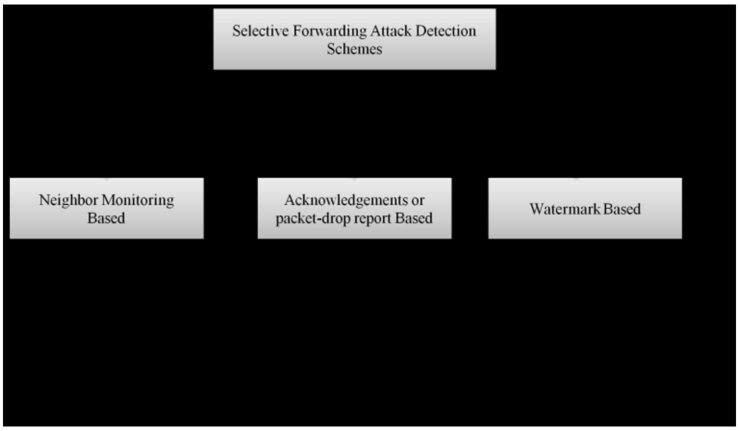
Selective Forwarding Attack Detection Schemes
Neighbor Monitoring Based
Acknowledgements or packet-drop report Based
Watermark Based

Figure 1: Classification of Selective Forwarding Attack Detection Schemes

The aforementioned detection schemes can be either Centralized or Distributed. In the centralized schemes the responsibility to counter the selective forwarding attack lies only with the base station/cluster head. The other sensor nodes within the network do not participate in the process. The distributed schemes, in contrast to centralized schemes, involve the participation from the other senor nodes within the network to collaborate with the base station/cluster head to counter the attack. The major advantage of schemes exhibiting centralized behaviour is they have less energy overhead as compared to the distributed schemes. Also the network lifetime is more because the centralized schemes do not put much burden on the sensor nodes to counter the attacks as compared to the distributed schemes where the sensor nodes also participate in the counter process. The drawback of the centralized schemes is single point of failure, i.e. base station (BS)/ cluster head. If the cluster head is compromised, in case of the clustered sensor networks, or the base station gets surrounded by the malicious node thus preventing the base station from getting the attack reports, the entire countermeasure fails. The distributed schemes, on the other hand, have the advantage of improved detection accuracy, low false alarm rates and also if the cluster head gets compromised or the base station gets surrounded by the malicious nodes, the other sensor nodes within the network can still detect the attack and isolate the malicious node. But these schemes have high energy consumption rate as well as communication overhead.

IV. literature review

The overview of the previous research work in the area of detecting the Selective Forwarding attack in wireless sensor networks is described below:

4.1. Selective Forwarding Attack Countermeasures:

4.1.1 Detecting Selective Forwarding Attacks in Wireless Sensor Networks [6]

Bo Yu et al. proposed a lightweight distributed detection scheme which attempts to detect the occurrence of the selective forwarding attack using multi-hop acknowledgement technique and also identifies the malicious node responsible for the attack. All nodes on the data flow path participate in the detection process. The multi-hop acknowledgement scheme is used to launch the alarms by obtaining the responses from the intermediate sensor nodes. Upon detecting the misbehavior of the downstream (upstream) nodes, the in-between sensor node generates an alarm packet and delivers it to the source node (the base station) using multiple hops, where downstream represents the direction towards the base station and upstream represents the direction towards the source node. The BS and the source node then use IDS (Intrusion Detection System) algorithms to make the decision. The detection process is reliable and efficient in the sense that the intermediate sensor nodes will report any abnormal packet loss and the malicious nodes to both the base station and the source node.

4.1.2 Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks [2]

Suk-Bok Lee et al. proposed an efficient and reliable counter scheme based on the Neighbor Watchdog System (NWS) to identify the malicious behavior of the packet dropper node in the network. The scheme works on single-path data forwarding and converts into multi-path data forwarding upon detection of malicious activity in the network by NWS. The number of multipath depends upon the number of sub-watch nodes around the malicious node. If no malicious packet dropping is detected en-route to the base station within the network by NWS, the data packet is forwarded along the single path only. Each relay node forwards the data packet to a node in its neighbor list and if it fails to do so, the watch nodes forwards the packet to their next hop. The simulation results have shown that the scheme achieves a high success ratio in the presence of large number of packet dropping nodes and adjusts its forwarding style depending upon the number of the dropper nodes on the route to the destination.

4.1.3 Detecting Selective Forwarding Attacks in Wireless Sensor Networks using SVMs [7]

Sophia Kaplantzis et al. proposed selective forwarding attack detection scheme which utilizes Support Vector Machines (SVMs) and sliding windows technique. The scheme is centralized in nature which means the responsibility of detecting the attack and the malicious node lies solely with the base station. The authors have used a simple classification based IDS (Intrusion Detection System) to detect the selective forwarding attack in the WSN. The scheme is able to detect other attacks as well. The scheme uses the routing information which is local to the base station and based on the 2D feature vector (bandwidth, hop count), the alarms are raised. Classification of the data patterns is done using a one-class SVM classifier. The authors have simulated the application in which the goal of the deployed network is to report the BS about the presence of the attacker within the network, as quickly as possible. This is achieved by the sensors sensing the movement of vehicle in their surroundings and reporting the data back to the BS. From the packets the BS is able to get the information about the vehicle movement pattern and its status. The authors have used Minimum Transmission Energy (MTE) routing protocol to forward the packets from the source node to the BS. The authors have preferred

SVMs over other traditional classification methods, like neural networks and nearest neighbor classifiers, because SVMs are capable to provide very good results, even for very difficult training tasks, while avoiding the problems of overfitting and dimensionality. The scheme is able to detect selective forwarding attacks and the black hole attacks with the high accuracy rate without burdening the sensor nodes or reducing the network lifetime.

4.1.4 Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Two-Hops Neighbor Knowledge [8]

Tran Hoang Hai et al. proposed a detection scheme that uses the neighbor monitoring technique and the two-hop neighbor knowledge to detect the selective forwarding attack and its types in WSN. The authors have used two- hop neighbor knowledge as a part of their attack detection process to ensure that the neighbor node to which the current node forwards the relaying packet is actually the neighbor of the current node and lies on the right path to the sink. The scheme is distributed in nature which means the sensor nodes collaborate to detect the presence of the attack. Each sensor node in the network is equipped with the detection module built on the application layer and is responsible to passively detect the selective forwarding attack in its neighbor node. This detection scheme, like many other existing schemes, takes advantage of the broadcast nature of the sensor networks. The nodes within the intersection of radio ranges of the source and the destination monitor their neighborhood and raise alerts when the attack is detected. The authors have used the over-hearing mechanism for MAC (medium access control) layer to reduce the number of redundant alert packets sent to the base station.

4.1.5 CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attacks in Wireless Sensor Networks [9]

Young Ki Kim et al. proposed a selective forwarding attack detection scheme that does not require time synchronization and one-way key chains to detect the presence of attack. The scheme can detect the selective forwarding attack and can also identify the malicious node used by the attacker to launch the attack. The authors have used the Cumulative Acknowledgements to be sent to the base station when the intrusion is detected. The cumulative acknowledgements are sent to the base station and not towards the source node and thus the authentication is accomplished with the pre-distributed keys between the base station and the sensor nodes. The scheme consists of three phases: Topology construction and Route Selection, Data Transmission, and Detection Process. The authors have used SEEM protocol for topology construction and route selection which is a secure routing protocol against sinkhole attacks and, thus, this scheme is able to detect sinkhole attacks as well.

4.1.6 Lightweight Defense Schemes against Selective Forwarding Attacks in Wireless Sensor Networks [10]

Wang Xin-sheng et al. proposed distributed selective forwarding attack detection scheme based on the hexagonal WSN mesh technology. The scheme employs neighbor monitoring technique to monitor the packet transmission of neighbor nodes and then resends the packet dropped by the dropper to the destination node. The scheme consists of two phases: Routing discovery and Data Transmission with attack defense. Within the routing discovery phase the number of hops on the shortest path from the source node to the destination node are determined and the source node forwards the event packet to the next hop selected using the routing algorithm (OPA_uvwts). The in-between nodes are responsible for packet forwarding and the monitor nodes are responsible for monitoring the intermediate node. If selective forwarding attack is detected it resends the packet to the destination and raises alarm to its neighbors informing them the location of the malicious node.

4.1.7 Detecting Selective Forwarding Attacks in WSNs using Watermark [11]

Deng-yin ZHANG et al. proposed Digital Watermarking technology based centralized selective forwarding attack detection scheme for wireless sensor networks. The watermark is embedded into the data packets originated from the source and is extracted at the base station and packet dropped and modified rate calculated. The base station is responsible for identifying whether the node is malicious or not by analyzing the packet loss rate calculated from the received data. The scheme is implemented in location –based routing protocol GPSR and uses the safety value associated with each node to identify the malicious node and select the forwarding path. Base station manages the safety values of the nodes in the network and updates them using the fast-reduce and slow-growth principle. If the node is identified as malicious node, its safety value is fast-reduced by the base station, and if not, then the base station executes slow growth principle every T-clock cycles. The safety value of the node i, is initialized to 1. When the BS suspects a node i as malicious node, the BS will decrease its safety value and when the number of times a node i detected as malicious node exceed predefined threshold, the BS will declare node as the malicious node and revoke it from the network.

4.1.8 A Provenance based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks [12]

Salmin S. et al proposed centralized watermarking based scheme to detect the selective forwarding attack within the network and to detect and isolate the malicious node as well. The major goal of the scheme is to detect the packet dropping attack and then to detect the malicious node utilizing this provenance transmission technique. The authors have used **Data Provenance** as a tool to detect the attack and identify its source. The authors utilized the inter-packet delay based scheme is implemented in clustered sensor networks running LEACH protocol. The scheme works in three phases: Packet Loss Detection, Identification of Attack Presence, and Localizing Malicious Node/Link. The process is initiated by the BS (Base Station) for each sensor data flow and then waits for sufficient number of packet losses. The BS then calculates the average packet loss rate and compares it with the natural packet loss rate to identify the attack. Upon the detection of attack, the BS alerts the source node and the intermediate nodes to start the mechanism of isolating the malicious node.

Table 2: Summary of Selective Forwarding Attack Detection Schemes

Scheme	Other Attacks Countered	Special Features	Limitation
Bo Yu et al [6] (2006)	None	First paper to give detailed mechanism to detect selective forwarding attack; attacks detected even when the BS surrounded by malicious nodes.	Increased Communication overhead; energy parameter not considered; delay in packet-forwarding; lack of immediate action [6]
S.B. Lee et al [2] (2006)	None	Scheme can secure any routing protocol in senor network, normally follows single-path forwarding; upon detection of malicious behavior converts into multi-path forwarding. Implemented on LEAP protocol; provide defense against the attacks ranging from basic selective forwarding attack to blind letter attack	Storage overhead exists; scheme requires encrypting relaying packet with cluster key of a forwarding node so that all its neighbors can decrypt and overhear it.
Sophia K. et al [7] (2007)	Blackhole attacks	First paper to apply Support Vector Machines as a solution to WSNs; Blackhole attacks detected with 100 % accuracy; selective forwarding attack with approx 85 % accuracy.	Cannot identify the malicious node and revoke it [9];
Tran Hoang et al [8] (2008)	Blind Letter attacks	Reduces communication overhead and energy consumption using overhearing mechanism to send alert packets to base station.	Assumed static topology, requires pre-distribution pair-wise key management to prevent outside attackers.
Young Ki Kim et al [9] (2008)	Sinkhole attacks	First scheme to identify malicious nodes launching selective forwarding attack without broadcast authentication; Used 7 different scenarios to explain the detection process; Time synchronization not required; Cumulative acknowledgements sent towards base station rather than source node.	Predefined topology construction using SEEM protocol
Wang Xin-sheng et al [10] (2009)	None	No need to determine number of attackers in advance; event packets not lost when attack occurs; takes immediate action upon detecting attack.	Lower storage overhead; lower communication overhead because of single path forwarding; fixed topology: WSN mesh topology,
Deng Z. et al [11] (2011)	None	The method detects malicious nodes which dropped or modified packets, detection process starts only when malicious node exists	No packet retransmission mechanism provided, one malicious node detected at a time
Salmia et al [12] (2011)	None	The base station is able to detect the dropped packets, the malicious node dropping the packets as well as the packets modified by the malicious node	Power usage increases by 0.06%

Table 4: Analysis of Selective Forwarding Attack Detection Schemes

Scheme	**Class of Scheme**	**Detection Approach Used**	**Security Feature**	**Evaluation Metrics used**	**Time synchro-nization needed**	**Reliable Delivery in presence of attack**	**Energy overhead**	**Outcomes**
Bo Yu et al [6]	Distributed	Multihop ACK based	Attack+ malicious node detection	Alarm reliability, undetected rate, relative communication overhead	Yes	✓	High	Detection accuracy over 95% when channel error rate @ 15%
S. B. Lee et al [2]	Distributed	Neighbor Monitoring Based	Attack + malicious node detection	Success ratio (% of packets successfully reaching BS)	No	✓	Average	High packet delivery ratio in presence of large number of malicious nodes
Sophia K. et al [7]	Centralized	One class SVMs (Support Vector Machines) & sliding windows	Attack detection only	false alarm rate	No	×	Average	Blackhole detection rate=100%, selective forwarding attack detection=85%
Tran Hoang et al [8]	Distributed	Neighbor monitoring Based	Attack detection only	Packet delivery ratio, detection rate, power consumption	No	×	High	Detection rate=80%
Young Kim et al [9]	Centralized	ACK based	Attack + malicious node detection	Communication overhead, detection accuracy	No	×	High	Successful detection without broadcast authentication
W. Sheng et al [10]	Distributed	Neighbor monitoring Based	Attack + malicious node detection	Packet delivery ratio, average energy consumption	No	✓	Average	Detection with 100% packet delivery ratio
Deng Z. et al [11]	Centralized	Watermark Based	Attack + malicious node detection, detects modified packets	Detection rate vs. packet dropped rates, Detection rate vs. packet modified rate	No	✓	Low	Detection rate 95% approx when packet loss rate below 10%
Salmin S. et al [12]	Distributed	Watermark based data provenance	Attack + malicious node detection, detects modified packets	Detection rate, energy efficiency	No	✓	Average	High detection rate, power usage increases by 0.06%

V. Conclusion

The selective forwarding attack is a serious threat to the security of the sensor networks since it is hard to detect, especially when the attacker includes itself on the path of data flow. This paper presents a brief overview of the selective forwarding attack and the detection measures against it in the wireless sensor networks. The literature survey presented here gives a brief idea of the research done in this area and gives the knowledge about the existing security mechanism against the attack.

As understood from the analysis table, some schemes provide better detection rate but no mechanism to assure data delivery in presence of the attack, while some schemes provide better detection accuracy and reliable data delivery but high on energy consumption. In future, work can be done towards developing a scheme which is energy efficient and can detect as well as prevent the attack with greater accuracy while providing the reliable data delivery. Also, the selective forwarding attack exploits the network natural packet loss such as congestion and so if we can somehow able to detect if the packets are dropped due to congestion or malicious activity, detecting the malicious node will become more efficient.

References

[1] Chris Karlof and David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Ad Hoc Networks, 1(2-3), 2003, 293-315.

[2] Suk-Bok Lee and Yoon-Hwa Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, Proc. 4th ACM Workshop. on Security of Ad Hoc and Sensor Networks, San Francisco, CA, 2006, 59-70

[3] Xie-Lei, Xu Young-jun, Pang Yong, Zhu Yue-Feil, A Polynomial Based Countermeasure to Selective Forwarding Attack in Sensor Networks, WRI International Conference on Communications and Mobile Computing, 2009,455-459.

[4] Hae Young Lee and Tae Ho Cho,Fuzzy-Based Reliable Data Delivery for Countering Selective Forwarding Attack in Sensor Networks, Proc. 4th International Conference on Ubiquitous Intelligence and Computing, Springer-Verlag, 2007, 535-544.

[5] H. Sun, C. Chen and Y. Hsiao, An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks, Proc. IEEE TENCON, October 2007, 1-4.

[6] Bo Yu and Bin Xiao, Detecting Selective Forwarding Attacks in Wireless Sensor Networks, 20th International Parallel and Distributed Processing Symposium, 2006,1-8.

[7] Sophia Kaplantzis, A. Shilton, N. Mani and Y. Sekercioglu, Detecting Selective Forwarding Attack in Wireless Sensor Networks using Support Vector Machines, 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP), 2007,335-340.

[8] Tran Hoang Hai and Eui-Nam Huh, Detecting Selective Forwarding Attack in Wireless Sensor Networks using Two-Hops Neighbour Knowledge, 7th IEEE International Symposium on Network Computing and Applications, 2008, 325-331.

[9] Young Ki Kim, Hwaseong Lee, Kwantae Cho and Dong Hong Lee, CADE: Cummulative Acknowledgement Based Detection of Selective Forwarding Attacks in Wireless Sensor Networks, 3rd International Conference on Convergence and Hybrid Information Technology, 2008, 416-422.

[10] Wang Xin-sheng, Zang Yong-Zhao, Xiong Shu-ming and Wang Liang-min, Loghtweight Defense Scheme Against Selective Forwarding Attacks in Wireless Sensor Networks, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009,226-232.

[11] Deng-yin Zhang, Chao Xu and Lin Siyuan, Detecting Selective Forwarding Attacks in WSNs using Watermark, International Conference on Wireless Communication and Signal Processing, 2011,1-4.

[12] Sultana S., Bertino E. and Shehab M., A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks, International Conference on Distributed Computing Systems Workshops, 2011,332-338.