# Survey: Detection Schemes Against Selective Forwarding Attack

**Harpal Singh**[1], **Vaibhav Pandey**[2]

[1]Department of Computer Science & Engineering, PTU (Main Campus), Kapurthala, India

[2]Department of Computer Science and Engineering, PTU (Main Campus), Kapurthala, India

**Abstract:** ***Wireless sensor network becomes increasingly popular with the development in technology. It can provide enormous amount of services for the benefit of mankind. But due to its limitations in memory and other resources it is very much prone security attacks, selective forwarding attack is one that security attacks which can affect the whole sensor network communication. The variety of defense scheme has been proposed against selective forwarding attack. In this paper we have describe some of the existing defense scheme against selective forwarding attack.***

**Keywords:** Selective forwarding attack, Wireless sensor, Network, security, Distributed, Centralized.

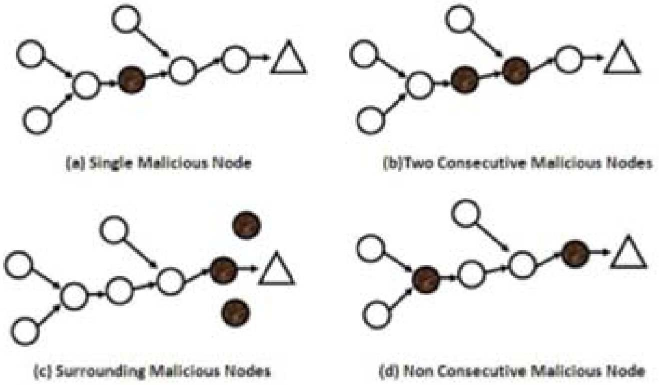
## 1. Introduction

In today's fast running world technology is growing each day. Recent advances in digital electronics, wireless communications, and micro-electro-mechanical systems (MEMS) technology enabled us to develop small sized sensor nodes that have a multi-function like sensing, data processing, and wireless communication. These small sized multi-functional nodes can deploy cooperatively to construct wireless sensor network. WSN is emerging as an interesting and promising area. Wsn has proved its utility in number of field in the present world. Wsn is mostly deploying in military field, medical, disaster management and home security systems. Integrated into number of devices, Machines, and environments, sensor provide number of social benefits. They can help to avoid catastrophic infrastructure failures, save precious natural resources, increase productivity, enhance security systems, and enable new applications such as context-aware systems and smart home technologies. But it can be prone to number of security attacks like selective forwarding attack which can be very harmful in mission critical application and affect whole communication system. It is very difficult to detect because of its nature, in this attack node work normally but refuse to forward selected packet and drop them or pass to some other sources.

This paper is an effort to analyse selective attack and all the defence scheme to counter it .The main objective of this paper is to give the overview of existing defence scheme against selective forwarding attack. We have made an attempt to cover all drawbacks and advantages of existing countermeasures against selective forwarding attack.

## 2. Selective Forwarding Attack

The selective forwarding attack was first introduced by Karloff and Wagner [1]. It is also called as Gray Hole attack Selective forwarding is a denial of service attack which affect the routing data at the network layer , in selective forwarding attack compromised node refuse to forward particular packet on the route to the base station selectively. This attack can be launch by placing malicious node in the routing path which have similar capability of nodes in the network .It can also be launch with the help of sinkhole and wormhole attack. We can categorise selective forwarding attack on the basis of malicious node count in routing path and on the basis of type of packet it drop [2].



(a) Single Malicious Node

(b)Two Consecutive Malicious Nodes

(c) Surrounding Malicious Nodes

(d) Non Consecutive Malicious Node

**Figure 1:** [2] Categorization Of Selective Forwarding based on node count in routing path in WSN.

Based on the packet it drop selective forwarding attack can be considered into following two types.
1. Drop packet of some specified node.
2. Drop packet of some specified type

## 3. Categorizations of Previous Scheme against Selective Forwarding Attack

The scheme to counter selective forwarding attack can be categorize according to two types of criteria [3].
1. Nature of scheme
2. Defense of scheme

Nature of scheme of scheme and defense of scheme can be further classified as follows:

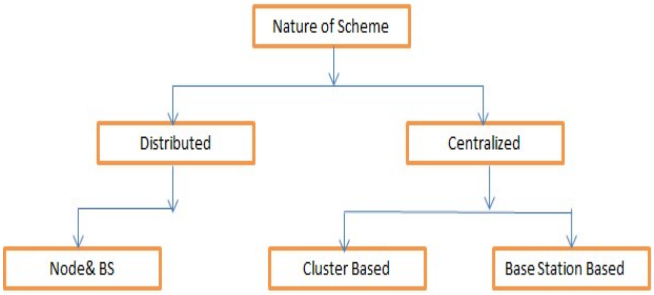


**Figure 2:** Classification of selective forwarding attack by nature of Scheme.

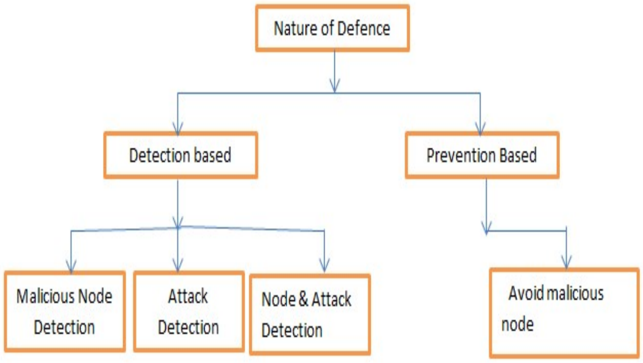


**Figure 3:** Classification by defence of Scheme

## 4. Schemes against selective forwarding attack and countermeasures

The overview of the existing detection scheme against selective forwarding attack is described below.

### 1)"Secure routing in wireless sensor networks: attack and countermeasures".

Karloff et.al [1] was first to introduced the selective forwarding attack and also suggest multi-path routing as countermeasures to tackle these type of attacks. According to this scheme, message routed over n path through completely disjoint nodes, it provide some probabilistic protection over n compromised node. It uses multiple braided paths which may provide more protection against selective forwarding attack. In this scheme node probabilistically choose next hop from set of possible candidate, which can further reduced the chance of losing control to adversary.

Draw Backs of Scheme.

- It has very poor security resilience , adversary need to place only one malicious node in each path
- Does not bother about detection of malicious node and notification about attack to neighbor.
- Energy consumption increase with increase in path.
- No implementation of specific method for detection of attack.

### 2) "Lightweight Defense scheme against selective Forwarding Attack in Wireless sensor network".

This scheme is proposed by Xin-sheng et al [4]. According to this scheme sensor network is divided into hexagonal mesh topology, in each hexagonal there can be only one node is active for the operation. Each node find its geographical location through GPS and find which hexagonal it belong to , node neighbour to this node is set as monitor node which keep close look at each operation of node when any event is occur .The neighbour node monitor the transmission of packet through routing path if any node in routing path drop packet monitor node mark that node as malicious node and change the path of packet to ensure the delivery to the sink. This scheme is very energy efficient as only one node can be activated in each hexagonal cell and also it ensure the proper delivery of data to the base station. There are some limitations of this scheme. This scheme doesn't explain some important aspect.

Draw Backs of Scheme.

- If there is any change in topology, this may affect the performance of scheme as it is assumed that after development the nodes will not change their location.
- Use of GPS to find location make network costly.
- If monitor node will compromised no countermeasures is proposed to deal with it.
- On detection of malicious node doesn't explain whether to remove complete cell or particular node.

### 3)"Detecting Selective Forwarding Attack in Wireless Sensor Networks using SVMs".

K. Sophia et al [5] have proposed a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and have used sliding windows for black hole attacks and selective forwarding attacks. In this particular scheme they only detect the attacks. They also claimed that, this is the first attempt to apply SVMs as a solution in a WSN security. This scheme raises alarm based on the 2D feature vector (bandwidth, hop count) by using routing information local to the base station of the network .Classification of the data patterns is performed using a one-class SVM classifier[5]. They use anomaly detection as base for their scheme. Anomaly detection signals an intrusion when the observed activities differ significantly from those usually undertaken by the user. The authors consider a minimum energy routing protocol, called minimum transmission energy (MTE). Their scheme can detect black hole attacks with 100% accuracy and selective forwarding attacks with 85% accuracy. In this scheme intrusion detection is performed in the base station and hence the sensor nodes use no energy to support this added security feature.

Draw Backs of scheme.

- This particular scheme detects the execution of selective forwarding attack only but cannot identify malicious nodes or find alternate paths.
- The centralized based detection in scheme suffer from single node failure problem, means if the centralized node is compromised then the whole network will suffer.

### 4)"Fuzzy-Based Reliable Data Delivery for Countering Selective forwarding attack in wireless sensor network".

Hea Young et al [6] have proposed a Fuzzy based reliable data delivery scheme to detect the selective forwarding attack which is an improved version of Multi-path routing method. The improvement is that the number of routing path varies with number of attacker. They are both using a redundant strategy such that the event packet is transmitted in multiple paths. Fuzzy logic is used to determine the number of paths for data delivery by considering the energy level of the node in the network and the number of malicious nodes. The proposed scheme uses the propagation limiting method as a means for routing if multi-path routing is insufficient for reliable data delivery. They have also assumed that the base station know or estimate the energy level of network and the number of malicious nodes in advance and that all the nodes know their location. Multi-hop acknowledgement scheme [3] is also used for selective forwarding attack detection.

Draw Backs of Scheme.

- Limitations are similar with Multi-path routing method but it but it detects number of attacker in advance.
- Energy consumption is more because of redundant transmission.
- Scheme cannot identify the malicious node and poses more overhead to the network due duplicate packet.

### 5) "Detecting Selective Forwarding Attack in Wireless sensor Networks Using Two-hop Neighbour Knowledge".

Tran Hoang et al [7] have proposed a centralized cluster based lightweight detection technique to detect selective forwarding attack in WSNs. This scheme is based only on 2-hops neighborhood information and over-hearing technique. In this scheme each sensor node is equipped with a detection module built on application layer. Detection module is responsible to detect the selective forwarding attack in its neighbor node. The detection scheme depends on the broadcast nature of sensor communication and takes benefits of high density of sensors deployed in the sensed environment. . The sensor nodes which activate the detection module called as monitor nodes. In this scheme as a part detection mechanism each node stores two-hop neighbor list. Each sensor node associates each neighbor node with a malicious counter. The malicious counter can be defined as the threshold of abnormal activity of a sensor node which cannot exceed. When malicious counter is crossed the threshold, it revokes the malicious node from its direct neighbor list.

Draw Backs of Scheme.

- No mechanism is proposed if the monitoring node or cluster head is compromised.
- In case of change in topology, this scheme will not work because the authors have assumed that the topology is static.
- No countermeasure is taken to handle selective forwarding attack and reliable data transmission.

### 6) CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attack in Wireless sensor Networks".

Young Ki Kim et al [8] have proposed a Centralized based scheme called CADE Cumulative Acknowledgement based Detection of selective forwarding attacks. It detects malicious nodes which cause selective forwarding attack without the need for time synchronization. This scheme can also detect sinkhole attack. This scheme sends cumulative acknowledgments to the base station not to the sources node, and hence authentication is accomplished with pre-distributed keys between the base station and nodes. CADE 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.

Draw Backs of Scheme:

- If topology change, this scheme will not work as topology is pre-defined this scheme.
- Consume large amount of energy due to topology construction and route selection.
- Due to centralized nature of this scheme, it faces single node failure problem, for example if base station will compromised network will goes down.
- The scheme identifies malicious node only, so countermeasures need to be accompanied with this scheme for reliable retransmission of drop data packets.

### 7) "Detection of Selective Forwarding Attack in Heterogeneous sensor Networks".

Jeremy Brown et.al [9] have proposed a centralised cluster based scheme for detecting the selective forwarding attack in sensor network by using Wald's Sequential Probability Ratio Test(SPRT) method[9].This scheme use powerful high-end sensor and this is bases on the sequential probability ration test .The scheme detect attack with high detection ratio and very low false alarm rate. Each node listens passively for the transmission packet, if any node downstream node drop the packet, the upstream node will observe the packet drop. The monitor node (L-sensor) will send the report packet to cluster head (an H-sensor), the report include the node ID of the dropper. Bases on this report packet, a powerful H-sensor performs the sequential probability ratio test and determines if an L-sensor is compromised or not.

Draw backs of Scheme.

- If cluster head is compromised scheme will not work hence face single node failure problem.
- There is no mechanism proposed for reliable retransmission of drop packet.
- This scheme only detects the malicious node but mechanism needs to be developing for reliable retransmission of drop packets.

### 8) "Polynomial-based Countermeasures to Selective Attack in Sensor Networks".

Xie lei et al [10] has proposed a polynomial based scheme to detect selective forwarding attack, a security scheme use redundant data to tolerate the loss of critical packets. This scheme split the sensing data into parts and sends these parts instead of the original sensing data to the sink by using a dynamic individual path forwarding mechanism so that, forwarding node cannot understand the contents of the data generated by the polynomial, which can minimise the possibility of eavesdropping. When data reached at sink, it can parse the original event data and if the malicious node tampers with data, sink can detect the tampering of data.

There are some assumptions made by the author like the network consists of static sensor nodes and sink having knowledge about topology and it trusted entity in the network and cannot be compromised. Each node in the network shares a unique symmetric key with the trusted sink.
Draw Backs of scheme.

- Scheme will not work properly if the topology change and in case base moves from its location or compromised.
- Cause extra computational and storage overhead to divide and process the original data packet.
- More communication overhead by sending polynomial value to the sink.

### 9)"Detecting Selective Forwarding Attack Using Watermark in WSNs".

Deng et al [11] have proposed a centralized detecting method by watermark using the trust value in the routing selected protocol. They made improvement in the geographic forwarding protocol by combining the trust value with distance to choose an optimal data forwarding path. They use a watermark based scheme is used to detect selective forwarding attack. When attack is detected, detection mode starts. Malicious node can be detected and addressed during this detection mode. Detection accuracy of this scheme is over 95% even with 10% channel error rate. There are some assumptions made by the author like base station is always trusted and cannot be compromised. Each node has trust value which is maintained by the base station. At beginning all nodes in the network has the same trust value and all of trust values change dynamically.
Draw Backs of Scheme.

- Unable to detect more than one malicious node in the packet forwarding path.
- Data retransmit method need to be proposed.

### 10) "CHEMAS: Identify suspect nodes in Selective Forwarding Attack".

Xiao, Yu and Gao [12] have proposed a technique for detecting malicious nodes in selective forwarding attack. They have actually improved their previous technique for detection of selective forwarding attack and named it as CHEMAS (checkpoint-based multi-hop acknowledgement scheme). In this scheme they randomly choose part of intermediate nodes along a forwarding path as checkpoint node. The checkpoint nodes are responsible for generating acknowledgements packet for each event 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 has the potential to detect abnormal packet loss and identify suspect nodes if it does not receive enough acknowledgements from the downstream checkpoint nodes
Draw Backs of scheme.

- More energy is consumed in sending acknowledgement packet, alarm packet.
- Require more storage space due to us e of one-way hash key.
- Does not guaranty reliable packet transmission in case of packet dropping.
- Require node to be loosely synchronise with base station.

### 11) "An Efficient Countermeasures to the Selective Forwarding Attack in Wireless Sensor Networks".

Hung-Min Sun et al [13] have proposed a multidataflow topologies (MDT) method to detect the selective forwarding attack. The authors divide the sensor nodes into two-dataflow
topologies by using MDT, both dataflow topology can cover the monitored area, therefore the base station only requires one report from either topology to control the entire network. Through these two topologies the sink can defend against the selective forwarding attack. If a malicious node exists in one topology, the sink can still obtain packets from other topology. To locate a malicious node, the authors deploy the sensor nodes region by region during the deployment phase. Sensor nodes can be located in a range of some regions. When the sink loses some packets, it will mark all possible regions that the malicious sensor nodes may be deployed in. After that, the sink can gather and analyse the information about all possible lost regions; hence the sink can utilize the information to locate the malicious sensor nodes.
Draw Backs of scheme:

- Limited ability to detect the malicious node .Attacker can destroy the whole network by placing malicious node in each path.
- Scheme unable to identify compromised node efficiently and poses more communication overhead since it sends duplicate packet to sink.

### 12) "Game Theory Model for Selective Forwarding Attacks in Wireless Sensor Networks".

Yenumula B Reddy et al [14] have proposed scheme which use a framework to detect malicious nodes using Zero-Sum game approach and selective node acknowledgements in the forward data path. They have formulated the attack-defence game as a 2 player, nonzero-sum, non-cooperative game, and have shown that it achieves Nash equilibrium, thus leading to a defence strategy for the network, and significantly increasing the chance of detecting intrusions. In an attack model, two players are involved namely the intruder and detection system. The IDS at the node level maintains a table that stores the history of the packet drop rate, the selection of alternate routes, and enforcement of security levels. The IDS Calculates the payoff at the node level before packet transfer takes place from source (node) to destination (base station). If the payoff function bends towards the attacker, it means the node is compromised (the packet may be dropped). The cluster head or sink that monitors a similar situation at all nodes identifies all such compromised nodes and isolates them from the network. When a node is removed from the cluster, the transmission to/from that node will be ignored. Draw backs of scheme.

- Because of congestion and packet dropping accuracy of scheme suffer a lot.
- Unable to control packet dropping.

## 5. Future Scope

In this paper we review all existing technique to detect selective forwarding attack; future scope of this study is to provide the researchers all the drawbacks of existing schemes so that they can develop better and efficient detecting scheme.

## 6. Conclusion

As wireless sensor network is emerging field which has some mission critical application where loss of small amount of data may cause big damage, selective forwarding attack drop packet selectively which make it difficult to detect and defend. Researcher must proposed scheme in such a manner that it can differentiate the packet loss by malicious node and by transmission error, congestion. It should not cause overhead to network also consider the energy as an important objective which may increase the life of network.

## References

[1] C.Karlof and D.Wagner, "Secure routing in wireless sensor Networks: attacks and countermeasures", in Ad Hoc Networks, Vol.1, No.2, 2003, pp.293-315.

[2] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. An efficient countermeasure to the selective forwarding attack in wireless sensor networks. Oct.2007.

[3] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, "Comprehensive Study of Selective Forwarding Attack in Wireless sensor Networks" I.J.Computer Network and Information Security, 2011, 1-10MECS.

[4] 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.

[5] S.Kaplantzis,A. Shilton,N.Mani and Y. Sekercioglu, "Detecting Selective forwarding attack in Wireless Sensor Networks Using Support Vector Machines" in 3rd Conf. of Intelligent Sensor Networks and Information Processing,Dec.2007,pp.335-340.

[6] Hae Young, Tae Ho C.Fuzzy-Based reliable data delivery for countering Selective forwarding attack in Sensor Networks. Hong Kong, China, Springer-Verlag, 2007, p.535-544.

[7] Tran Hoang Hai,Eui-Nam, "Detecting Selective Forwarding attack in WSN Using Two-hops Neighbour Knowledge" 7th IEEE International Symposium on Network Computing and Application 2008,pp.325-331.

[8] Y.Ki Kim, Hwaseong Lee, Kwantae Cho, D. Hoon Lee, "CADE: Cumulative Acknowledgement based Detection of Selective Forwarding attacks in WSNs"3rd International Conference on Convergence and Hybrid Information Technology,2008,pp.416-422.

[9] J.Brown and X. Du, "Detection of Selective forwarding attack in heterogeneous sensor networks", in International Conf. on Communications, May 2008,pp.1583-1587.

[10] Xie Lei, Xu Yong-Jun, Pan Yong, Zhu Yue-Feil, ,"A Polynomial based Countermeasures to Selective Forwarding Attack in WSNs"International Conference on Communications and Mobile .

[11] Deng-yin,Chao,Lin Siyuan, "Selective forwarding attack Detection using Watermark in WSNs"International Colloquium on Computing ,Communication, Control, and Management(2009 ISECS),pp.109-113,2009,pp.445-459.

[12] 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.

[13] H.Sun, C.Chen and Y.Hsiao, "An efficient Countermeasures to the selective forwarding attack in wireless sensor Networks", in IEEE TENCON 2007, Oct.2007, pp.1-4.

[14] Y B Reddy, S.Srivathsan, "Game Theory Model for Selective forwarding attack in Wireless sensor Networks" 17th Mediterranean Conference on control & Automation Makedonia Place,Thessaloniki,Greece june 24-26,2009,pp.458-463.

## Author Profile

**Harpal Singh** received the B-Tech degree in Computer Science & Engineering from Giani Zail Singh College of Engineering and Technology, Punjab Technical University Campus, Bathinda in 2012, currently he is doing M-tech in computer science & Engineering (Networking System) from PTU Main Campus, his research area is wireless sensor network.

**Vaibhav Pandey** received B. Tech. degree in Computer Science & Engineering from Uttar Pradesh Technical University, Lucknow, India. He has done M.Tech. from National Institute of Technology, Hamirpur, India. His research areas are wireless sensor network and distributed computing.