I.J. Computer Network and Information Security, **2011, 1, 1-10**
Published Online February 2011 in MECS (http://www.mecs-press.org/)

Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks

Wazir Zada Khan
School of Computer Science
Jazan University, Saudi Arabia
wazirzadakhan@yahoo.com

Yang Xiang
School of Information Technology
Deakin University, Australia
yang@deakin.edu.au

Mohammed Y Aalsalem
School of Computer Science
Jazan University, Saudi Arabia
aalsalem@jazanu.edu.sa

Quratulain Arshad
School of Computer Science
Jazan University, Saudi Arabia
brightsuccess_12@yahoo.com

Abstract **— Sensor networks are becoming closer towards wide-spread deployment so security issues become a vital concern. Selective forwarding attack is one of the harmful attacks against sensor networks and can affect the whole sensor network communication. The variety of defense approaches against selective forwarding attack is overwhelming. In this paper we have described all the existing defensive schemes according to our best knowledge against this attack along with their drawbacks, thus providing researchers a better understanding of the attack and current solution space. This paper also classifies proposed schemes according to their nature and defense. Nature of scheme classifies into Distributed and Centralized. Defense of scheme classifies into detection and prevention.**

Index Terms **— Selective Forwarding Attack, Sensor Network, Security**

I. INTRODUCTION

Sensor Networks first came into eminence in the late 1990s with the advent of Motes device [1, 2], and the TinyOS operating system [3]. Wireless Sensor Networks are modernizing the way the people interact with the physical world. They comprise of small sensor nodes which have many capabilities such as sensing, monitoring, computation and wireless communications. They are deployed in large amounts to collect data from the environment, perform local processing and communicate their results. In this paper, we investigate the Selective Forwarding Attack and its variants, which is very simple to implement but difficult to detect. In selective forwarding attack the malicious node works as a normal node but refuses to forward certain selected packets and simply drop them. So, due to this nature, the selective forwarding attack is very harmful for mission critical applications and can damage the whole network communication, making the network useless.

This paper is the first effort towards the systematic analyses of the Selective Forwarding attack and its all existing defenses in sensor networks. The main objective of this research paper is to give an overview for all those researchers and developers who used to propose different techniques to counter Selective Forwarding attack. The developers may make this paper a source when developing techniques for detecting and defending against selective forwarding attack as this paper covers all the drawbacks of existing countermeasures for selective forwarding attack.

II. Selective Forwarding Attack and its Variants

The selective forwarding Attack was first described by Karlof and Wagner [2]. This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them.

There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming form a particular node or a group of nodes. This behavior causes a **DoS attack** for that particular node or a group of node.

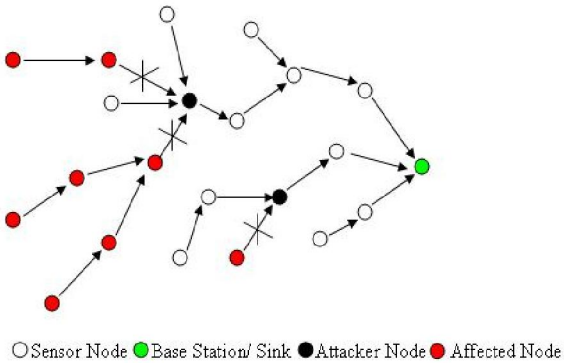


Figure 1. Example of Selective Forwarding in form of Dos attack

They also behave like a Blackhole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network. Another form of selective forwarding attack is called Neglect and Greed. In this form, the subverted node arbitrarily neglecting to route some messages [1]. It can still participate in lower level protocols and may even acknowledge reception of data to the sender but it drops messages randomly. Such a node is neglectful. When it also gives excessive priority to its own messages it is also greedy. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between sensor nodes. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between sensor nodes.

Figure. 2 below shows how the selective forwarding attack works through a simple example. The selective forwarding attack may be happened in the link from node S to node A in several ways. In the path to the sink, node S forward or send the packets to its neighbor node A but node A stop forwarding the packets from node S. Otherwise, node A may forward the packet to an unknown malicious node through a high-quality route for eavesdropping [2].

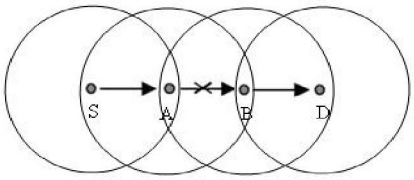


Figure 2. Example of Selective Forwarding attack

One more form of selective forwarding attack is referred to as **Blind Letter attack [19]**.The concept of this attack is that with arbitrarily malicious nodes, it should be guaranteed that the node, to which the next-hop node forwards the relaying packet, is really a neighbor of the next-hop node.

For example, node u forwards a packet to compromised node v, and node u listens in on node v's traffic to compare each overheard packet with the packet in the buffer. Node v transmits the relaying packet whose intended next-hop id marked with any id in the network such as x that is not a neighbor of v. Then node u overhears this packet from node v, and considers it forwarded correctly despite the fact that none actually receives the packet. The packet is eventually dropped without being detected. Selective forwarding attack is easy to implement, especially when the malicious node is included on the path of data flows. Selective forwarding attack can affect a number of multi-hop routing protocols, shown in the Table I.

TABLE I. List of Multi-hop Routing Protocols [2]

Multi-hop Routing Protocols
TinyOS beaconing
Directed diffusion and its Multipath Variant
Geographic Routing (GPSR, GEAR)
Minimum Cost Forwarding
Clustering based protocols (LEACH, TEEN, PEGASIS)
Rumor Routing
PSFQ
DSR

III. Related Work:

G.Padmavathi et al [12] have discussed a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced. The authors have described the selective forwarding attack and classify the selective forwarding attack as an active routing attack.

IV. Classification of Previous Schemes against Selective Forwarding Detection and Countermeasures:

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

A. Distributed and Centralized

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

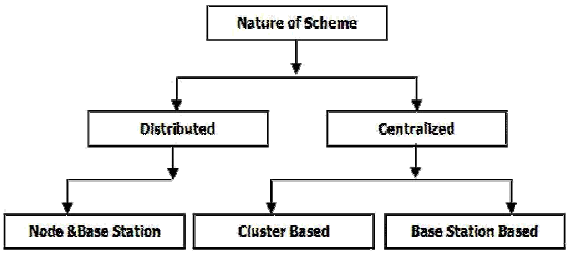


Figure 3. Classification by nature of schemes

B. Detection and Preventions:

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

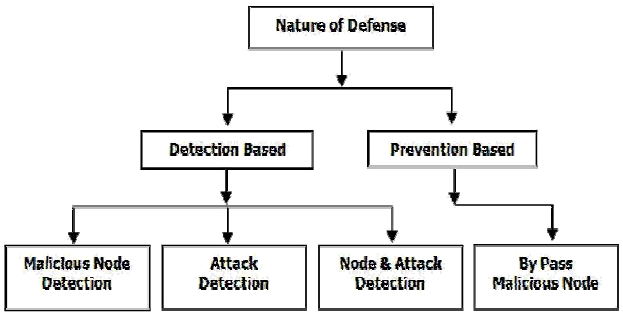


Figure 4. Classification by defense of schemes

V. Schemes against Selective Forwarding Detection and Countermeasures:

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

1. Secure routing in wireless sensor networks: attacks and countermeasures

Karlof et al. [2] first time discuss the selective forwarding attack and also suggest that Multi-path routing can be used to counter these types of attacks. Messages routed over n paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most n compromised nodes and still offer some probabilistic protection when over n nodes are compromised. The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. 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.

Draw Backs of Scheme:

1. Poor Security Resilience if there exists at least one node in the path[17]
2. No detection of malicious node and no notification about attack to neighbors [16,13]
3. Increase in energy consumption when the number of paths increase.[16]
4. Increase in Network flow and communication overheads. [8,13]
5. No implementation of specific method for detection of attack and attacker.

2. Detecting Selective Forwarding Attacks in Wireless Sensor Networks

Yu and Xiao [3] have proposed a distributed detection scheme that uses multi hop acknowledgements from intermediate nodes to raise alarms in the network. Their scheme focuses on selective forwarding attack in which detection occurs in both the base station and source nodes.

In this scheme, each intermediate node along the forwarding path is in charge of detecting malicious nodes. If an intermediate node detects the misbehavior of its downstream (upstream) nodes, it will generate an alarm packet and deliver it to the source node (the base station) through multiple hops. The base station and the source node can then use more complicated IDS (Intrusion Detection System) algorithms to make decisions and responses. The authors have used routing and transport protocols such as Directed Diffusion [20] and PSFQ [21].

Draw Backs of Scheme:

1. The nodes may involve more multi-hop response acknowledgements to detect selective forwarding attack, and choose another path to retransmit the packet successfully resulting in certain delay and communication overhead. [13, 14]
2. Lack of efficiency. Sensor nodes in this scheme take much effort to detect the selective forwarding attack.
3. Security problem. This scheme cannot detect the attack successfully in some particular condition.
4. Lack of scalability. This scheme only considers the selective forwarding attack. Hence, WSN needs other countermeasures if suffering other kinds of attacks [6].
5. The members of a checkpoint list (acknowledge node) can be predicted, therefore making part of the intermediate nodes the target of compromising [4].

3. CHEMAS: Identify suspect nodes in selective forwarding attacks

Xiao, Yu and Gao [4] have proposed a technique for identifying suspect 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 select part of intermediate nodes along a forwarding path as checkpoint nodes which 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 has the potential to detect abnormal packet loss and identify suspect nodes if it does not receive enough acknowledgements from the downstream checkpoint nodes.

TABLE II: Qualitative Analysis of Schemes

Technique/ Scheme	Type (Detection/ Prevention)	Counter other Attacks	Claimed Accuracy	Scheme Nature	Consider Other means of Packet dropping	Routing Protocol Used	Simulation Tool Used	Multi-Path Based	Acknowledge-ment Based	Neighbor Monitoring	Reliable Data Delivery
Karlof et al 's Scheme[2]	Prevention	Yes	-	Distributed	No	-	-	Yes	No	No	Yes
Yu and Xiao 's Technique [3]	Detection	No	95%	Distributed	Yes	DD, PSFQ	-	No	Yes	No	No
CHEMAS [4]	Detection	No	95%	Distributed	Yes	DD, PSFQ	-	No	Yes	No	No
Support Vector Machines Based Technique [5]	Detection	Yes	80%	Centralized	No	MTE	OMNET++	No	No	Yes	No
Hung-Min Sun et al 's Scheme [6]	Prevention	No	-	Centralized	No	-	-	No	No	No	Yes
Krontiris et al ' Scheme [7]	Detection	Yes	96.75%	Distributed	No	-	-	No	No	Yes	
Fuzzy-Based Reliable Data Delivery Scheme [8]	Prevention	No	100%	Distributed	No	DD	-	Yes	No	No	Yes
Two-hops Neighbor Knowledge Based Scheme [9]	Detection	No	90%	Distributed	Yes	-	Castalia	No	No	Yes	No
CADE [10]	Detection	Yes	-	Centralized	No	SEEM	-	No	Yes	No	No
Jeremy Brown et al ' Scheme [11]	Detection	No	80%	Centralized	Yes	-	Custom C Based	No	No	Yes	No
Watermark Based Technique [13]	Detection	NO	95%	Distributed	Yes	GF	-	No	No	No	No
A Polynomial-Based Scheme [14]	Prevention	No	-	Distributed	No	GF	-	No	No	No	No
Chanatip et al 's Scheme[15]	Detection	Yes	100%	Centralized	No	-	Visual Sense	No	No	Yes	No
Wang Xin-sheng et al 's Scheme [16]	Detection	No	100%	Distributed	No	OPA_uvw ts	NS-2	No	No	Yes	Yes
Game Theory Model Based Scheme [17]	Detection	No	-	Centralized	No	-	Matlab	No	Yes	No	No
A Sequential Mesh Test based Scheme [18]	Detection	No	-	Centralized	No	-	-	No	No	Yes	No
Suk-bok et al 's Technique[19]	Detection	No	-	Distributed	No	LEAP	NS-2	Yes	No	Yes	Yes

Draw Backs of scheme:

1. By using one-way hash key chains for authentication for each packet requires storage space [10, 16].
2. More energy is consumed by sending acknowledgement, alert packets include one-way hash key [9,10,16, 18]
3. No guarantee for reliable transmission of packet in case of packet dropping [16].
4. It requires nodes to be loosely time synchronized [10].

4. Detecting Selective Forwarding Attacks 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 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 uses routing information local to the base station of the network and raises alarms based on the 2D feature vector (bandwidth, hop count). Classification of the data patterns is performed using a one-class SVM classifier. 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). In MTE, the next hop is chosen such that the transmission energy expended by the sending node is minimized, in an attempt to extend each individual node's lifetime. They have detected selective forwarding attack in a sensor network by using one-class SVM and chosen the one-class approach based on the fact that they are unlikely to know the form of any attack a-priori, and hence any attack training set they could construct, would be unlikely to provide an accurate representation of any actual attack on the network.

Draw Backs of Scheme:

1. This scheme only detects the execution of selective forwarding attack but unable to identify malicious nodes or find alternate paths. Thus, another countermeasure should be accompanied with this scheme [9, 10].

2. The centralized based detection techniques suffer from single node failure problem, means if the centralized node is compromised then the whole network will suffer.

5. An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks

Hung-Min Sun et al [6] have proposed a multi-dataflow topologies (MDT) method to countermeasure the selective forwarding attack. By using MDT the authors divide the sensor nodes into two-dataflow topologies, 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 two topologies the base station can defend against the selective forwarding attack. If a malicious node exists in one topology, the base station can still obtain packets from other topology. For locating a malicious node, the authors deploy the sensor nodes region by region during the deployment phase. 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. After that, the base station can gather and analyze the information about all possible lost regions; hence the base station can utilize the information to locate the malicious sensor nodes.

Draw Backs of scheme:

1. The scheme ability to resist the attacks is very limited, when there is a malicious node in each path, the attacker can completely destroy data transmission, and communication overhead is not improved.[14]
2. Scheme cannot identify compromised nodes efficiently and there is an increased communication overhead since it sends duplicate packets. [10].

6. Towards Intrusion Detection in Wireless Sensor Networks

Krontiris et al. [7], have defined a Distributed Intrusion Detection Scheme (IDS) for sensor networks based on watchdogs for selective forwarding and sinkhole attacks. They have adopted specification based rules and cooperative decision making techniques to create IDS with low false positives and false negative alarms. Neighbor monitoring is used for detecting selective forwarding attack in sensor networks. Watchdog approach [21] is used by neighboring nodes which can easily monitor the behavior of a node to see whether it forwards correctly the packets it receives. By adopting specification-based approach, they define which norms are going to be used to describe normal operation. These specifications for detecting black-hole and selective forwarding attacks can simply be a rule on the number of messages being dropped by a node. Each of the watchdog nodes will apply that rule for itself to produce an intrusion alert. The naive approach would be to increment a counter every time a packet is dropped and produce an alert when this value reaches a threshold.

Draw Backs of scheme:

1. Not an efficient scheme as the final decision will be taken after all the alerts are received from all the neighbors.
2. No energy measurements are included in the simulation of this solution [5].
3. This scheme cannot detect if the packet is forwarded to the right path to the sink [9]

7. Fuzzy-Based Reliable Data Delivery for Countering Selective Forwarding in Sensor Networks

Hea Young et al [8] have proposed a Fuzzy based reliable data delivery scheme for countering selective forwarding attack which is an improved form of Multi-path routing method. The enhancement is that the number of transmission path varies with number of attacker. They are both using a redundant strategy such that the event packet is transmitted in multiple paths. The number of paths for data delivery is determined by a fuzzy logic with consideration of the energy level of the network and the number of malicious nodes. The proposed method 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:

1. This scheme has the same limitations as Multi-path routing method. In addition, it has to determine the number of attackers in advance.[16]
2. Redundant transmission of packets and scarce energy resources are unnecessary consumed. [16]
3. This scheme cannot identify compromised nodes and increase communication overhead since they send duplicate packets. [10]

8. Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge

Tran Hoang et al [9] have proposed a centralized cluster based lightweight detection technique to detect selective forwarding attack and its variance in WSNs. This scheme is based only on 2-hops neighborhood information and over-hearing technique. Each sensor node is equipped with a detection module built on application layer. Detection module is responsible to passively detect the selective forwarding attack in its neighbor node. The detection mechanism relies on the broadcast nature of sensor communication and takes advantage of high density of sensors deployed in the sensed environment. . The sensor nodes activate the detection module called monitor nodes. They also apply two-hop neighbor knowledge as a part of their detection technique and 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. The authors have made some assumptions like no node can be trusted and the neighbor node knowledge is secure and confidential in the deployment time and finally they have assumed that the network has a static topology and requires a pre-distribution pair-wise key management to prevent outside attackers.

Draw Backs of Scheme:

1. No way out is proposed if the monitoring node or cluster head is compromised.
2. In case of change in topology by any means, the scheme will not work as the authors have assumed that the topology is static.
3. No countermeasures are taken for selective forwarding attack and reliable data retransmission is not assured.

9. CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attacks in Wireless Sensor Networks

Young Ki Kim et al [10] have presented 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. Their scheme also provides security against sinkhole attack. Their scheme sends cumulative acknowledgments to the base station not towards 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 [22] protocol for topology construction and route selection. Through different scenarios they have shown the detection of malicious node.

Draw Backs of Scheme:

1. In case of change in topology by any means the scheme will not work as the topology is pre-defined.
2. The scheme is not energy efficient due to its topological construction and route selection and data reply message through multi paths.
3. The centralized based detection techniques suffer from single node failure problem, means if the base station is compromised then the whole network will suffer.
4. This scheme only identifies malicious nodes so countermeasure should be accompanied with this scheme for reliable retransmission of drop data packets.

10. Detection of Selective Forwarding Attacks in Heterogeneous Sensor Networks

Jeremy Brown et al [11] have presented a centralized cluster based scheme for detecting the selective forwarding attack in sensor networks by applying Wald's Sequential Probability Ratio Test (SPRT) method [23]. The scheme utilizes powerful high-end sensors and is based on the sequential probability ratio test. 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 down-stream 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 (an H-sensor). Based on the reports, a powerful H-sensor performs the sequential probability ratio test and determines if an L-sensor is compromised or not. All the results are proved through a customize simulator written in C.

Draw Backs of Scheme:

1. Single node failure problem in case if the Cluster Head is compromised.
2. No mechanism is proposed for reliable retransmission of drop packets.
3. This scheme only identifies malicious nodes so countermeasure should be accompanied with this scheme for reliable retransmission of drop data packets.

11. Selective Forwarding Attack Detection using Watermark in WSNs

Huijuan Deng et al [13] have proposed a centralized detecting method by watermark technology using the trust value in the routing selected algorithm. They have improved geographic forwarding algorithm by combining the trust value with distance to choose an optimal data forwarding path. A watermark-based scheme is used to detect the selective forwarding attack. When such an attack is detected, detection mode starts. The malicious node can be detected and addressed. The simulating results show that even when the channel error rate is 10%, the detection accuracy of the proposed scheme is over 95%. The authors have made some assumptions like the base station is always trusted and can not be comprised by the adversary. Every node has a trust value. The base station stores and manages the trust value of each node. The nodes of the entire network have the same trust value at the beginning of the network initialization and all of the trust values change dynamically. The malicious nodes only drop some of the packets.

Draw Backs of Scheme:

1. This scheme is unable to detect more than two malicious nodes in the path, so the second malicious node will be found by the next time detection which leads to an extra over head.
2. No data retransmission method is described after packet is dropped.

3. The assumption, dropping of packets only by malicious node and base station can not be compromised, make this approach not suitable for real sensor networks.

12. A Polynomial-based Countermeasure to Selective Forwarding Attacks in Sensor Networks

Xie Lei et al [14] have proposed a polynomial modeling based countermeasure against selective forwarding attack and a security scheme using redundant data to tolerate the lost of critical event messages. The basic idea is to split the sensing data into parts and to send these parts instead of the original sensing data to the sink by adopting a dynamic individual path forwarding mechanism so that , the forwarding nodes can not understand the contents of the data generated by the polynomial, which can prevent eavesdropping . When the sink received enough parts, it can parse the original event data and if the malicious nodes tamper with data, the sink can detect the tampered data. The authors have made some assumptions like the network consists of static sensors nodes and the sink knows the topology and it is trusted powerful entity in the network and can not be compromised. Finally, before the sensor nodes are deployed, every node shares a unique symmetric key with the trusted sink.

Draw Backs of Scheme:

1. Change in topology and in case if the base station moves from its location or compromised then the scheme will not work accurately.
2. Dividing and processing the original data packet into small sizes leads to extra Computational and Storage Overhead
3. The communication overhead comes mainly from sending polynomial values to the sink.

13. Detecting Sinkhole Attack and Selective Forwarding Attack In Wireless Sensor Networks

Chanatip et al [15] have proposed a Traffic Monitor Based Selective Forwarding Attacks Detection Scheme. Their approach uses EM nodes to eavesdrop and monitor all traffics of the network. The authors also introduced a scheme for sinkhole attack based on Received Signal Strength Indicator (RSSI) readings of messages. They have used RSSI value from four EM nodes to determine the position of all sensor nodes which the Base Station (BS) is origin position (0, 0). They have focus on an address based selective forwarding attack in which, the attacker selectively drops packets based on the source address. As a result, the attacker causes DOS for those nodes only, while remaining normal for all the other nodes. The authors have also taken some assumptions like at the beginning; there is a static network, where all nodes are immobile after initial deployment. Secondly the attackers can physically displace or remove some of sensor nodes from their original positions to some extent to modify the target area monitored by these sensors if the attackers attempt to avoid being detected by the sensor network or deceive the network. Finally, they have assumed that the BS and EM nodes are physically protected or have tamper-robust hardware.

Draw Backs of Scheme:

1. Any change in topology will affect the efficiency of the scheme.
2. The may suffer from single node failure problem as due to the assumption that the BS and EM nodes are physically protected or has tamper-robust hardware

14. Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks

Wang Xin-sheng et al [16] have presented a distributed lightweight defense scheme against selective forwarding attack, which is based on a hexagonal WSN mesh topology. This scheme utilizes the neighbor nodes to monitor the transmissions of the event packet and detect selective forwarding attack by monitoring packets' forwarding of two nodes in the transmission path, and resend these packets dropped by the attackers to the destination node. The event packet is forwarded according to the routing calculated by the routing algorithm (OPA_uvwts) from source to destination. The intermediate node is responsible for forwarding the event packet. The monitor node is responsible for the detection of possible selective forwarding attack and if selective forwarding attack is identified, it retransmits the event packet to the destination node and finally when selective forwarding attack is detected, it sends an alarming message to its neighbor nodes for notifying the location of attacker thus avoiding the attacker node in forwarding the incoming packets. The authors have made some assumptions for network model like after deployment; location of the nodes does not change any more. Secondly the active node can listen to packets from one hop node. Finally during the process of event packet transmission from the source node to the destination node, the packet may suffer from selective forwarding attacks.

Draw Backs of Scheme:

1. If there is any change in topology, it will affect the performance of scheme as it is assumed that after development the nodes will not change their location.
2. No countermeasure is proposed if in case the monitoring node is compromised.

15. Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks

Yenumula B Reddy et al [17] have proposed a framework to detect malicious nodes using Zero-Sum game approach and selective node acknowledgements in the forward data path. The authors have formulated the attack-defense game as a 2-player, nonzero-sum, non-cooperative game, and have shown that it achieves Nash equilibrium, thus leading to a defense 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:

1. The accuracy of the detection will severely suffer due to congestion and other causes of packet dropping.

16. A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks

Guorui Li et al [18] have proposed the sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks. The scheme nature is centralized and works for cluster based sensor networks. The sensor node sends the packet drop report message through another path to the cluster head if it doesn't observe the forwarding data message from the next hop sensor node in a fixed interval. The cluster head runs the sequential mesh test based detection scheme against the suspicious node after receiving the packet drop reports. Then sequential mesh test [24] extracts a small quantity of samples to run the test, instead of regulating the total times of test in advance. It decides whether continue the test or not based on the test result until it obtains the final conclusion. In order to detect the selective forwarding attack, wireless sensor nodes should listen promiscuously to the network after sending their data packets. If the sender node hasn't observed the forwarding message after a fixed period of time, it can suspect that the intermediate relay node has dropped its packet. Then the sender node will report packet dropping event to the cluster head through another route. The detection scheme is based on the sequential mesh test method [24] which is basically hypothesis test and depending upon the ratio of packet drop the cluster head decides that the a particular node launching the selective forwarding attack or not. But the detection accurate ratio of the detection scheme becomes acceptable when the attack package drop rate is higher than the normal package drop rate.

Draw Backs of Scheme:

1. Although the detection of selective forwarding attack depends upon the ratio of packet drop but this detection is not accurate (not satisfy able) because when the attack package drop rate is lower than the normal package drop rate. The reason lies in the fact that the normal package drop events have severe influence on the selective forwarding attack detection.
2. The scheme also suffers when the cluster head is comprised as there is no countermeasure given for this. The scheme also suffers from single node failure problem.

17. A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks

Suk-bok et al [19] have proposed a resilient packet-forwarding scheme using Neighbor Watch System (NWS) against maliciously packet-dropping nodes in sensor networks. This scheme basically employs single-path data forwarding, which consumes less power than multi-path schemes. The packet is forwarded along the single-path towards the base station; however, the scheme uses multi-path data forwarding at the location where NWS detects relaying nodes' misbehavior. The watch node around a malicious node can find that after receiving, the malicious node do not transmit to other nodes or transmit to a node that does not exist in its neighbor list, and then the watch node must retransmit the package. This scheme is based on LEAP [20] protocols.

Draw Backs of Scheme:

1. As, it is necessary that each node broadcasts its neighbor's table and then stores the neighbor's table of its neighbors, which consumes more storage space. Moreover, the watch nodes need store packets around them for potential retransmit, which requires some buffer and energy consumption. [14]

VI. DISCUSSION

Both centralized and distributed schemes have pros and cons. Although prevention is a good approach but the malicious node still exist in the network and some other countermeasures must be taken to detect and remove them from network. On the other hand detection of malicious node scheme must be intelligent enough, so that they can distinguish between packet dropping by malicious node and other reasons like congestion, network failure, buffer full and bad radio conductions.

VII. CONCLUSION & FUTURE WORK

For many real time applications secure routing is critical to the acceptance and use of sensor networks. The definition and the existing work done by different authors are very important in understanding the threat and in proposing an effective scheme for detecting and preventing the selective forwarding attack. One more thing that the authors doing research in this area must consider is that their proposed schemes must be capable of perceiving the true causes of packet dropping that is it can distinguish that packets are dropping either due to congestion or by a malicious node. Also, it is of the

essence that the schemes or techniques proposed in future should be enough competent so that they can both detect and prevent the selective forwarding attack as an attack detection scheme itself cannot be an ultimate solution and prevention may be safer than relying on detection.. Winding up, almost all existing schemes have drawbacks hence; a very vigilant, efficient, economical and node cooperation based defensive mechanism is needed to counter the selective forwarding attack.

VIII. ACKNOWLEDGMENT

The authors wish to acknowledge the anonymous reviewers for valuable comments.

IX. REFERENCES

[1] *Anthony* Wood, John A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35(10):54-62, October 2002.

[2] 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.

[3] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. of the 2nd International Workshop on Security in Systems and Networks*, April 2006, pp. 1-8.

[4] 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.

[5] 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.

[6] H. Sun, C. Chen and Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in *Proc. Of IEEE TENCON 2007*, Oct. 2007, pp. 1-4.

[7] K. Ioannis and T. Dimitriou, "Toward intrusion detection in sensor networks," in *13th European Wireless Conference*, April 2007, pp.1-7.

[8] 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.

[9] 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.

[10] 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.

[11] J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks," in *International Conf. on Communications*, May 2008, pp. 1583-1587.

[12] G.Padmavathi, 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

[13] 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

[14] Xie Lei, Xu Yong-jun, Pan Yong, Zhu Yue-Fei1 ,"A Polynomial-based Countermeasure to Selective Forwarding Attacks in Sensor Networks" International Conference on Communications and Mobile Computing, 2009, pp.455- 459.

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

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

[17] Yenumula B Reddy, S. Srivathsan ,"Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks" 17th Mediterranean Conference on Control & Automation Makedonia Palace, Thessaloniki, Greece June 24 - 26, 2009, pp. 458-463

[18] 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.

[19] 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.

[20] S. Zhu, S. Setia, and S. Jajodia, LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, The 10th ACM Conference on Computer and Communications Security (CCS '03), 62-72, 2003

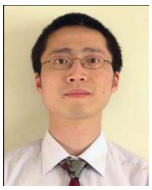
[21] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MobiCom '00)*, 2000, pp. 255–265.

[22] N. Nasser and Y. Chen, SEEM: Secure and energy efficient multipath routing protocol for wireless sensor networks, Computer Communications, Volume 30, Issue 11-12, pp. 2401-2412 , September 2007.

[23] N. Ahmed, S. S. Kanhere, and S. Jha, "Intrusion Detection Techniques for Mobile Wireless Networks," Mobile Computing and Communications Review, Vol. 9, No. 2, pp. 418, 2005.

[24] X. Pu, Z. Yan, S. Mao, Y. Zhang and Y. Li, "The sequential mesh test for a proportion," in *Journal of East China Normal University*, *No*. 1, 2006, pp. 63-71.

Wazir Zada Khan is currently with School of Computer Science, Jazan University, Kingdom of Saudi Arabia. He received his MS in Computer Science from Comsats Institute of Information Technology, Pakistan. His research interests include network and system security, sensor networks, wireless and ad hoc networks. His subjects of interest include Sensor Networks, Wireless Networks, Network Security and Digital Image Processing, Computer Vision.



Dr. Yang Xiang is currently with School of Information Technology, Deakin University. He received his PhD in Computer Science from Deakin University. His research interests include network and system security, distributed systems, and wireless systems. In particular, he is currently leading in a research group developing active defense systems against large-scale distributed network attacks and new Internet security countermeasures. His recent research has been supported by the Australian Research Council (ARC), the University, and industry partners. Dr. Xiang has published more than 100 research papers in international journals and conferences. He has served as Program/General Chair for many international conferences such as ICA3PP 11, IEEE/IFIP EUC 11, TrustCom 11, IEEE HPCC 10/09, IEEE ICPADS 08, NSS 11/10/09/08/07. He has been PC member for many international conferences such as IEEE ICC, IEEE GLOBECOM, Malware, and IEEE ICPADS. He is regular reviewer for many international journals such as IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Dependable and Secure Computing, IEEE Communications Letters, and IEEE Journal on Selected Areas in Communications. He is on the editorial board of Journal of Network and Computer Applications.

Dr. Mohammed Y Aalsalem is currently dean of e-learning and assistant professor at School of Computer Science, Jazan University. Kingdom of Saudi Arabia. He received his PhD in Computer Science from Sydney University. His research interests include real time communication, network security, distributed systems, and wireless systems. In particular, he is currently leading in a research group developing flood warning system using real time sensors. He is Program Committee of the International Conference on Computer Applications in Industry and Engineering, CAINE2011. He is regular reviewer for many international journals such as King Saud University Journal (CCIS-KSU Journal).

Quratulain Arshad received her BS in Computer Science from Comsats Institute of Information Technology, Pakistan. Her research interests include network security, trust and reputation in sensor networks and ad hoc networks. Her subjects of interest include Network Security, Digital Image Processing and Computer Vision.

